(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－191940

(43)公開日　平成７年(1995)７月28日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ｇ	7459－5L		
	Ｄ	7459－5L		

審査請求　未請求　請求項の数15　ＯＬ　（全 17 頁）

(21)出願番号　特願平5－332655

(22)出願日　平成５年(1993)12月27日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　廣瀬　浩一
鎌倉市上町屋325番地　三菱電機株式会社
コンピュータ製作所内

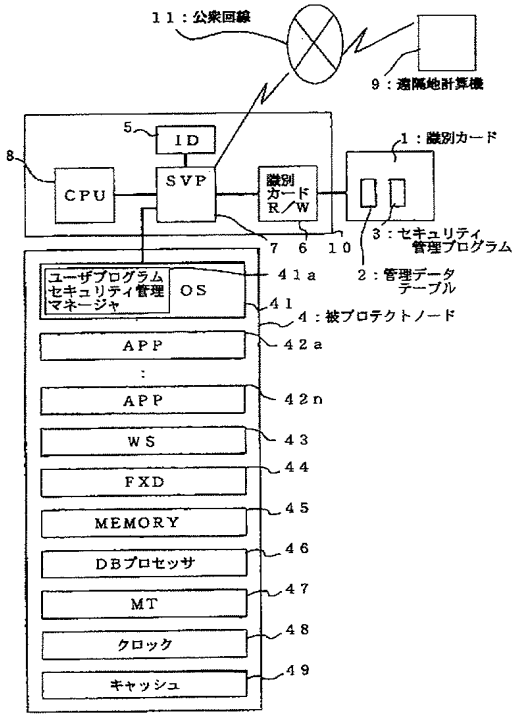
(74)代理人　弁理士　高田　守

(54)【発明の名称】　計算機の資源利用方式

(57)【要約】

【目的】　オプションＨ／Ｗ或は計算機Ｓ／Ｗの不法な使用を防止し、識別カードを使用することにより、管理データテーブルの不法改竄の抑止効果を向上させる。

【構成】　識別カード１の管理データテーブル２には、被プロテクトノード４（オプションのＨ／Ｗ、及びＳ／Ｗ）の使用可否、及び使用期限等のデータが入っている。システムたち上げ時にセキュリティー管理プログラム３とＳＶＰ７は計算機筐体に設けられた個別の識別子５と識別カード１に格納された個別の識別子との認証を行ない、指定された識別番号を送ってきた計算機に対してのみ管理データテーブルのアクセスを許可する。整合がとれなければそこで、システムたち上げを中止する。



1

【特許請求の範囲】

【請求項１】　以下の要素を有する計算機の資源利用方式

（ａ）計算機を個別に識別する識別子を計算機に格納する識別子格納手段、（ｂ）上記識別子と同一の識別子と、計算機が利用できる資源を被プロテクトノードとして定義した管理データテーブルを保持する識別カード、（ｃ）上記識別カードに保持された識別子を計算機に入力して上記識別子格納手段により格納された識別子と比較して、一致した場合に、計算機から上記識別カードに保持された管理データテーブルをアクセスし、計算機に対して管理データテーブルに定義された資源の利用を認める利用許可手段。

【請求項２】　上記利用許可手段は、計算機の起動時に、上記識別子格納手段により格納された識別子と上記識別カードに保持された識別子を比較して、管理データテーブルの内容を読みだし、読み出した管理データテーブルの内容を参照して計算機のシステム構成を決定するサービスプロセッサを備えたことを特徴とする請求項１記載の計算機の資源利用方式。

【請求項３】　上記サービスプロセッサは、識別カードから読み込んだ管理データテーブルの内容を記憶するとともに、記憶した管理データテーブルの内容を参照して使用するオペレーティングシステムをインストールするとともに、上記被プロテクトノードの起動要求に対して、被プロテクトノードの起動の可否を決定することを特徴とする請求項２記載の計算機の資源利用方式。

【請求項４】　上記識別カードは、アプリケーションプログラムを上記被プロテクトノードとして定義し、上記オペレーティングシステムは、アプリケーションプログラムの起動要求に対する管理データテーブルの参照をサービスプロセッサとの通信により行うセキュリティ管理マネージャを備え、セキュリティ管理マネージャが管理データテーブルを参照してアプリケーションプログラムの起動の許可を与えることを特徴とする請求項３記載の計算機の資源利用方式。

【請求項５】　上記識別カードは、接続端末を上記被プロテクトノードとして定義し、上記利用許可手段は、接続端末の接続制限をサービスプロセッサに行わせることを特徴とする請求項２記載の計算機の資源利用方式。

【請求項６】　上記識別カードは、ディスク記憶装置を上記被プロテクトノードとして定義し、上記利用許可手段は、ディスク記憶装置の接続制限をサービスプロセッサに行わせることを特徴とする請求項２記載の計算機の資源利用方式。

【請求項７】　上記識別カードは、主記憶装置容量を上記被プロテクトノードとして定義し、上記利用許可手段は、主記憶装置容量の接続制限をサービスプロセッサに行わせることを特徴とする請求項２記載の計算機の資源利用方式。

2

【請求項８】　上記識別カードは、接続データベースプロセッサを上記被プロテクトノードとして定義し、上記利用許可手段は、接続データベースプロセッサの接続制限をサービスプロセッサに行わせることを特徴とする請求項２記載の計算機の資源利用方式。

【請求項９】　上記識別カードは、テープ装置を上記被プロテクトノードとして定義し、上記利用許可手段は、テープ装置の接続制限をサービスプロセッサに行わせることを特徴とする請求項２記載の計算機の資源利用方式。

【請求項１０】　上記識別カードは、計算機クロック周波数を上記被プロテクトノードとして定義し、上記利用許可手段は、計算機クロック周波数の設定をサービスプロセッサに行わせることを特徴とする請求項２記載の計算機の資源利用方式。

【請求項１１】　上記識別カードは、キャッシュメモリを上記被プロテクトノードとして定義し、上記利用許可手段は、キャッシュメモリの設定をサービスプロセッサに行わせることを特徴とする請求項２記載の計算機の資源利用方式。

【請求項１２】　上記識別子格納手段は、識別子を書きかえ可能な不揮発性メモリに格納しサービスプロセッサの固有な手続きにより識別子を書換え可能としたことを特徴とする請求項１記載の計算機の資源利用方式。

【請求項１３】　上記計算機の資源利用方式は、少なくとも上記識別カードの識別子および管理データテーブルの内容のどちらか一方を計算機から更新できることを特徴とする請求項１記載の計算機の資源利用方式。

【請求項１４】　上記識別カードを、利用許可手段と独自に通信できる通信手段を有する専用不揮発性記憶媒体カードとしたことを特徴とする請求項１記載の計算機の資源利用方式。

【請求項１５】　識別カードと利用許可手段間を独自のインタフェースにより接続したことを特徴とする請求項１記載の計算機の資源利用方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、計算機において、ソフトウェアやハードウェア等の資源を利用するための計算機の資源利用システムに関するものである。特にロードするソフトウェア（以下、Ｓ／Ｗ）、あるいは接続するハードウェア（以下、Ｈ／Ｗ）に制限を与えるプログラムロード方式及びＨ／Ｗインストール方式に関するものである。

【０００２】

【従来の技術】セキュリティ機能を有する計算機システムについては、技術文献にしばしば見られる。例えば、特開平３－２３７５５１には、トランザクションシステムセキュリティ方法及び装置に関する内容が記述されている。上記技術は、システムコンポーネントの確認、ユ

ーザ識別の証明、ユーザ許可及びアクセス制御を識別カードを使用して実現しようとするものである。

【０００３】また、たとえば、特開平４－２５５０３０には、プログラムロード方式に関する内容が記述されている。上記技術は、制御プログラムを起動し識別コード入力装置から識別コードが入力されると、制御プログラムが、セキュリティ管理プログラムを起動し、そのセキュリティ管理プログラムにより実行可能なプログラムをロードするものである。

【０００４】

【発明が解決しようとする課題】上記技術は、主に被セキュリティプログラムとユーザとの認証をテーマとしており、ローカルに固有な計算機Ｈ／Ｗとそれに付随するＳ／Ｗ、周辺機器との認証まではカバーしない。上記技術における被セキュリティプログラム及び識別カードは複数のＨ／Ｗ上で同様に動作する。また、従来のセキュリティ機能を有する計算機システムは、計算機システムが既に持っている資源を、許可のないユーザによって使われてしまうことを防止するためのものである。あるいは、従来のセキュリティ機能とは、エンドユーザが他のユーザによって、許可なく使われてしまうことを防止するためのものである。一方、このようなエンドユーザのセキュリティ機能という観点とは異なる計算機の資源の利用制限を考える必要がでてきた。ソフトウェアの供給者あるいはハードウェアの供給者は、供給するソフトウェアやハードウェアが、契約された計算機のみで動作するような保証を得たいと考えている。すなわち、契約の対象となったソフトウェアや周辺機器等が契約した顧客の計算機のみで動作するようにし、ソフトウェアやハードウェアの不正使用を防止する必要がある。たとえば、販売されたソフトウェアが不正に他の計算機上で利用されたり、第三者が提供した周辺機器が、不正に計算機に増設されたりする場合があり、このような不正使用を防止する必要がある。

【０００５】この発明は、以上のような問題点を解決するためになされたもので、従来のエンドユーザのセキュリティ機能とは異なり、ソフトウェア提供者やハードウェア提供者に対して、提供したソフトウェアやハードウェアが不正に使用されることを防止する計算機の資源利用システムを提供することを目的としている。

【０００６】特に、本発明は、固有の当該計算機に対し、一対一に対応する識別カードを持ち、それぞれに固有のＳ／Ｗのロードの制限、あるいは周辺機器のインストールに制限を与える手段を提供するものである。

【０００７】具体的には、以下の目的を有している。

・資源（Ｈ／ＷおよびＳ／Ｗ）の利用は、顧客（マシン）毎に資源利用契約をしてもらう。

・ＩＣカードを利用した資源不正使用防止システムを構築する。ＩＣカードシステムを導入し、ＩＣカード中に、利用できる資源、及び、その有効期限等の情報を持ち、それに反する利用はできない仕組みを作りこみ、資源の不正使用を防止するシステムを構築する。

・ＩＣカード内の情報を、メーカ内に構築された顧客管理システムにも提供する。その情報を活用し、リプレースの促進、コンサルタント業務の徹底をはかる。また、ＩＣカード再発行時などは、顧客管理システム内の情報をもとにＩＣカードを複製する。

【０００８】

【課題を解決するための手段】請求項１記載の発明に係る計算機の資源利用方式は、以下の要素を有する。

（ａ）計算機を個別に識別する識別子を格納する識別子格納手段、（ｂ）上記識別子と同一の識別子と、計算機が利用できる資源を被プロテクトノードとして定義した管理データテーブルを保持する識別カード、（ｃ）上記識別子格納手段により格納された識別子と、上記識別カードに保持された識別子を比較して、一致した場合に、上記識別カードに保持された管理データテーブルをアクセスし、管理データテーブルに定義された資源の利用を認める利用許可手段。

【０００９】請求項２記載の発明に係る計算機の資源利用方式は、請求項１記載の計算機の資源利用方式において、上記利用許可手段が、計算機の起動時に、上記識別子格納手段により格納された識別子と上記識別カードに保持された識別子を比較して、管理データテーブルの内容を読みだし、読み出した管理データテーブルの内容を参照して計算機のシステム構成を決定するサービスプロセッサを備えたことを特徴とするものである。

【００１０】請求項３記載の発明に係る計算機の資源利用方式は、請求項２記載の計算機の資源利用方式において、上記サービスプロセッサが、管理データテーブルの内容、すなわち、計算機が利用する資源を被プロテクトノードとして記憶し、使用するオペレーティングシステムをインストールするとともに、上記サービスプロセッサは、上記被プロテクトノードの起動要求に対して記憶した管理データテーブルの内容を参照して被プロテクトノードの起動の可否を決定することを特徴とするものである。

【００１１】請求項４記載の発明に係る計算機の資源利用方式は、請求項３記載の計算機の資源利用方式において、上記被プロテクトノードをアプリケーションプログラムとし、オペレーティングシステムは、アプリケーションプログラムの起動要求に対する管理データテーブルの認証をサービスプロセッサとの通信により行うセキュリティ管理マネージャを備え、セキュリティ管理マネージャが管理データテーブルとの整合性をチェックしアプリケーションプログラムのロードの許可を与えることを特徴とするものである。

【００１２】請求項５記載の発明に係る計算機の資源利用方式は、請求項２記載の計算機の資源利用方式において、上記被プロテクトノードを接続端末とし、接続端末

の接続制限をサービスプロセッサに行わせることを特徴とするものである。

【００１３】請求項６記載の発明に係る計算機の資源利用方式は、請求項２記載の計算機の資源利用方式において、上記被プロテクトノードを接続ＦＸＤとし、接続ＦＸＤの接続制限をサービスプロセッサに行わせることを特徴とするものである。

【００１４】請求項７記載の発明に係る計算機の資源利用方式は、請求項２記載の計算機の資源利用方式において、上記被プロテクトノードを主記憶装置容量とし、主記憶装置容量の接続制限をサービスプロセッサに行わせることを特徴とするものである。

【００１５】請求項８記載の発明に係る計算機の資源利用方式は、請求項２記載の計算機の資源利用方式において、上記被プロテクトノードを接続データベースプロセッサとし、接続データベースプロセッサの接続制限をサービスプロセッサに行わせることを特徴とするものである。

【００１６】請求項９記載の発明に係る計算機の資源利用方式は、請求項２記載の計算機の資源利用方式において、上記被プロテクトノードを接続ＭＴとし、接続ＭＴの接続数制限をサービスプロセッサに行わせることを特徴とするものである。

【００１７】請求項１０記載の発明に係る計算機の資源利用方式は、請求項２記載の計算機の資源利用方式において、上記被プロテクトノードを計算機クロック周波数とし、計算機クロック周波数の初期設定をサービスプロセッサに行わせることを特徴とするものである。

【００１８】請求項１１記載の発明に係る計算機の資源利用方式は、請求項２記載の計算機の資源利用方式において、上記被プロテクトノードをキャッシュメモリとし、キャッシュメモリの初期設定をサービスプロセッサに行わせることを特徴とするものである。

【００１９】請求項１２記載の発明に係る計算機の資源利用方式は、請求項１記載の計算機の資源利用方式において、個別の識別子を、書きかえ可能な不揮発性メモリに格納しサービスプロセッサの固有な手続きにより識別子を書換え可能としたことを特徴とするものである。

【００２０】請求項１３記載の発明に係る計算機の資源利用方式は、請求項１記載の計算機の資源利用方式において、少なくとも上記識別カードの識別子および管理データテーブルの内容のどちらか一方を更新できることを特徴とするものである。

【００２１】請求項１４記載の発明に係る計算機の資源利用方式は、請求項１記載の計算機の資源利用方式において、上記識別カードを、サービスプロセッサとの特別な通信手段を有する専用不揮発性記憶媒体カードとしたことを特徴とするものである。

【００２２】請求項１５記載の発明に係る計算機の資源利用方式は、請求項１記載の計算機の資源利用方式において、識別カードとサービスプロセッサ間を独自のインタフェースにより接続したことを特徴とするものである。

【００２３】

【作用】請求項１記載の発明においては、識別カードを使用して資源の利用範囲を決定することができるので、あらかじめすべてのＨ／ＷおよびＳ／Ｗを納入しておきながらも、識別カード内で許可された利用範囲だけをユーザに使用させることができる。つまり、Ｈ／ＷおよびＳ／Ｗの納入媒体は１種類のものだけ用意すればよく、納入も１度ですむ。

【００２４】請求項２記載の発明においては、計算機の起動時に、管理データテーブルの内容を読み出すので、常に識別カードの内容を反映させたシステム構成の決定ができる。また、計算機の起動時に、識別カードで保証された管理データテーブルの内容に従ったオペレーティングシステムのインストールができる。

【００２５】請求項３記載の発明においては、計算機の起動時に、識別カードから読み出した管理データテーブルの内容をメモリーに記憶させ保持するので、サービスプロセッサは起動要求のたびに識別カードの読み込みのためのアクセスを行う必要がない。また、サービスプロセッサは、被プロテクトノードの起動要求に対して、その被プロテクトノードの起動の可否を決定するので、それぞれの被プロテクトノードを独立して、許可の対象とすることができる。また、識別カードの更新／メンテナンス等の時、システムからカードが取りはずされた時でも、アプリケーションプログラムのロードができる様になる。

【００２６】請求項４記載の発明においては、被プロテクトノードがオペレーティグシステムのもとで動くアプリケーションプログラムであるとき、オペレーティグシステムの中のセキュリティ管理マネージャが、管理データテーブルを参照し、アプリケーションプログラムの起動の可否をチェックし、そのアプリケーションプログラムのロードの許可を与えるので、識別カードの管理データテーブルの内容通りに各アプリケーションプログラム毎に許可の可否を決定することができる。

【００２７】請求項５記載の発明においては、被プロテクトノードが、計算機に接続される端末（ワークステーション、パーソナルコンピュータ等）であるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、その端末の利用の可否を決定する。

【００２８】請求項６記載の発明においては、被プロテクトノードが、計算機に接続されるディスク記憶装置であるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、そのディスク記憶装置の利用の可否を決定する。

【００２９】請求項７記載の発明においては、被プロテクトノードが、計算機に接続される主記憶装置であると

き、サービスプロセッサは、管理データテーブル内の情報を用いて、その主記憶装置の利用の可否を決定する。

【００３０】請求項８記載の発明においては、被プロテクトノードが、計算機に接続されるデータベースプロセッサであるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、そのデータベースプロセッサの利用の可否を決定する。

【００３１】請求項９記載の発明においては、被プロテクトノードが、計算機に接続されるテープ装置であるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、そのテープ装置の利用の可否を決定する。

【００３２】請求項１０記載の発明においては、被プロテクトノードが、計算機に利用される計算機クロック周波数であるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、その計算機クロック周波数の利用の可否を決定する。

【００３３】請求項１１記載の発明においては、被プロテクトノードが、計算機に接続されるキャッシュメモリであるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、そのキャッシュメモリの利用の可否を決定する。

【００３４】請求項１２記載の発明においては、計算機毎に個別である識別子を書き換え可能としたことにより、識別子が何も書き込まれていない計算機を出荷し、導入時に識別カードと同期をとって識別子を設定することが可能となる。

【００３５】請求項１３記載の発明においては、識別カードの内容の更新に際して、遠隔地からの通信手段によって計算機を介して識別子や管理データテーブルの内容を更新することができるので、新たなＳ／ＷやＨ／Ｗの使用に対する識別子や管理データテーブルの内容の更新時に客先に出向かなくともよい。また、遠隔から識別カードの不法改ざんや不正使用の監視が行え、二重のチェックとなる。

【００３６】請求項１４記載の発明においては、識別カードを、プロセッサ内蔵型のＩＣカードとして、ＩＣカード内のプロセッサによりＩＣカード内の情報をプロテクトすることができる。

【００３７】請求項１５記載の発明においては、プロセッサ内蔵型のＩＣカードでなく他の価格の安い媒体カードを利用可能する場合でも、識別カードとサービスプロセッサ間を独自のインタフェースとしたことにより、容易にデータにアクセスされないというセキュリティ機能を持たせることができる。

【００３８】

【実施例】

実施例１．まず、図１を用いて、この実施例の概略について説明する。図１はこの発明の一実施例のブロック図である。１は識別カード、２は被プロテクトノードを記述した管理データテーブル、３はセキュリティ管理プログラム、４は被プロテクトノード、５は計算機筐体に設けられた個別の識別子、６は識別カードリーダ／ライタ、７はＳＶＰ（サービスプロセッサ）、８は中央処理装置、９は遠隔地計算機、１０は計算機本体、１１は公衆回線である。

【００３９】識別カード１には被プロテクトノードを記述した管理データテーブル２とセキュリティ管理プログラム３が格納されている。管理データテーブル２には、被プロテクトノード４（オプションのＨ／Ｗ、及びＳ／Ｗ）の使用可否、及び使用期限等のデータが入っている。また、識別カード１内には、データの不法読み取り、不法改ざん防止の為、セキュリティ管理プログラム３が用意されており、ＳＶＰ７は管理データテーブルへのアクセスの際、識別カード１に固有の識別子を送らなければならない。識別カード１はその識別子の整合がとれた場合だけ管理データテーブルへのアクセスを許可する。セキュリティ管理プログラム３とＳＶＰ７は識別子認証を行い、セキュリティ管理プログラム３は指定された識別子を送ってきた計算機に対してのみ識別カード１の管理データテーブル２のアクセスを許可する。

【００４０】識別カード１の個別の識別子は計算機筐体に設けられた個別の識別子（たとえば、ＣＰＵ－ＩＤあるいは筐体番号）５と同一のものであり計算機据え付け時の起動で一回のみＳＶＰ７により識別カード１に書き込まれる。以降その個別の識別子がシステム立ち上げごとに認証に使用される。

【００４１】この動作を図２を用いて説明する。システムたち上げ時にシステムのコンフィグレーション或はイニシャルプログラムロードを行う際、筐体の識別子５、識別カードリーダ／ライタ６、被プロテクトノード４とインタフェースを持つＳＶＰ７は計算機筐体に設けられた個別の識別子５と識別カード１に格納された個別の識別子との認証をセキュリティ管理プログラム３を用いて行ない（Ｓ１）、整合がとれなければそこで、システムたち上げを中止する（Ｓ７）。

【００４２】整合がとれた場合（Ｓ２）、システムのコンフィグレーション或はオペレーティングシステムのイニシャルプログラムロードを行うが、ＳＶＰ７はその時の被プロテクトノード４の使用可否（Ｓ３）、使用期限（Ｓ４）を識別カード１の管理データテーブル２を通して知り、認証された内容に従って、インストレーション或はロードの行う（Ｓ５）。このチェックを管理データテーブル２に定義されたすべての被プロテクトノードについて行い（Ｓ６）、システムを立ち上げる。

【００４３】次に図３を用いて、ＯＳ（オペレーティングシステム）４１のもとで動くアプリケーションプログラム４２ａ～４２ｎが起動される場合のチェックについて説明する。ＳＶＰ７を通して、識別カード１内の管理データテーブル２との照合がオペレーティングシステム内のユーザプログラムセキュリティ管理マネージャ４１

ａによって行われ、許可されている場合はそのまま起動され、許可されていない場合は起動を中止される。また、ＳＶＰ７は遠隔地との通信機能を持つ。遠隔地計算機９は、公衆回線１１を通して遠隔地からの通信により、識別カード１へアクセスし、管理データテーブル２の更新を行う。

【００４４】次に、この実施例の詳細について、以下に説明する。なお、以下においては、識別カード１が、ＩＣカードであり、識別子を筐体番号として説明する。さらに、前述したユーザプログラムセキュリティ管理マネージャ４１ａをＳＶＣ（スーパーバイザーコール）インタフェースのチェックシステムコールで起動できるレーチンとして説明する。

【００４５】まず、システムの概要について述べる。

・ＣＰＵ－ＩＤ（筐体番号）と対になったＩＣカードがあり、正規のＩＣカードがセットされなければシステムは基本的には立ち上がらない。

・ＯＳがＩＣカードに格納されている管理データテーブルを読み出し、その内容に従って被プロテクトノードとして記憶された資源の機能をユーザに使用させるかどうか制御する。ＯＳが制御する主な内容は、以下のものである。

１）ＩＣカードにあるＯＳバージョン名とのチェックによるシステムの立ち上げの可否。

２）ＩＣカードにある使用を許可するＳ／Ｗとのチェックによる Ｓ／Ｗの起動の可否。

３）ＩＣカードにあるシステムＳ／Ｗの利用可能な有効期限とのチェックによるシステムＳ／Ｗの立ち上げまたは起動の可否。

４）ＩＣカードにある「同時に使用できる最大端末台数（あるいは、ＴＣＰ／ＩＰの論理リンク数）」とのチェックによる端末接続の可否。

５）ＩＣカードにある製品クラス情報にもとずく、製品クラスのチェック。

６）ＩＣカードにあるＳ／Ｗのバージョンとのチェックによる Ｓ／Ｗの立ち上げまたは、起動の可否。

【００４６】これらは、Ｓ／Ｗの不正使用を防止する目的で行うが、６）は他システムからのモジュールの不正なコピー防止を目的とするものである。このシステムでは、すべてのメーカ標準Ｓ／Ｗが、ＭＴ（マグネティクテープ）あるいは、ＤＡＴ（デジタルオーディオテープ）に格納された状態で客先へ出荷される。客先では、その内容物すべてを、ＯＳ専用領域を持つディスクへインストールする。ＯＳ専用領域は、ＭＴ内あるいはＤＡＴ内のＳ／Ｗ類、スワップ／ダンプ領域、および、各Ｓ／Ｗ独自に必要とするディレクトリを含み、将来性を考えた十分な大きさを持ち、大きさは固定とする。このＯＳ専用領域には、ユーザのプログラムやデータの格納を禁止する。

【００４７】次に、ＩＣカードのメモリ構造、および、メモリに書き込まれる情報について述べる。

［メモリ構造］メモリにはフラッシュメモリ（またはＥＰＲＯＭ等でもよい）が使用され、図４に示すようにシステム領域とユーザ領域の２つに大別される。

【００４８】［ＩＣカードに書き込むデータ］システム領域には、ＩＣカード自身の管理情報とユーザ管理情報が書き込まれる。

（１）ＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）

ＰＩＮは、利用者確認番号であり、この実施例では、システム設置後最初のＩＰＬ時にＰＩＮに筐体番号を設定し、次回以降のＩＰＬ時にＰＩＮを照合する。設定されたＰＩＮとＩＣカードが装着されたマシンの筐体番号を照合することにより、１つのＩＣカード内の情報（契約した資源を供給する情報）が特定のマシン以外では使用できないようにする。照合の結果が正しい場合には、ユーザ領域に設けられたＡＤＦ（Ａｐｐｌｉｃａｔｉｏｎ　Ｄａｔａ　Ｆｉｌｅ）の内容に従って資源単体毎に動作可否が決定され、不正の場合には縮退モードでのシステム稼働となる。

（２）ＩＣカード識別情報

ＩＣカード識別情報とは、ＩＣカードのＨ／Ｗ情報（メモリの種類や容量、ＩＣカード自身のバージョン、ＩＣカードのシリアル番号等）が書き込まれている。

（３）ユーザ管理情報

ユーザ（使用者）についての情報を管理するための領域であり、ＩＣカード発行の際にユーザ情報が営業部門のユーザ管理Ｄ／Ｂ（顧客管理データベースとも呼ぶ）をもとに書き込まれる。ユーザ管理情報の内容は図５に示すとおりである。

（４）ＡＤＦ（Ａｐｐｌｉｃａｔｉｏｎ　Ｄａｔａ　Ｆｉｌｅ）

ＡＤＦはＩＣカードのユーザ領域をアクセスする際の１つの単位で、ユーザ領域を使用するためには、初めにＡＤＦを作成（指定されたＡＤＦ－ＩＤに対応する領域をユーザ領域に確保）しなければならない。ＡＤＦを作成する際には、ＡＰＷ（ＡＤＦ毎のパスワード）とアクセス・レベルの指定が必要となる。

【００４９】ユーザ領域では、ＡＤＦ毎に分けて、メーカ側はＡＤＦの使用領域の管理とＯＳの核（カーネル）のもとで動くＳ／Ｗ（メーカ基本Ｓ／Ｗ）の管理を行い、ディーラではディーラ毎に決められた情報を管理する。以下、各管理情報毎に述べる。

（１）ＡＤＦ毎の使用領域管理情報：各ＡＤＦ毎の総バイト数と使用バイト数、空きバイト数の管理を行う。

（２）Ｓ／Ｗ管理情報：Ｓ／Ｗの管理を行い、Ｓ／Ｗ別の版名、使用開始日、有効期限、使用可否、製品クラス番号等の情報を管理する。図６を用いて具体的に説明する。図６において、ソフトウェアＩＤはソフトウェア毎の識別ＩＤである。つまり、同一ソフトウェアはすべて

11

同じ識別子を持っている。その識別子はソフトウェアの種類毎に固有であり、同じソフトウェアであれば共通の識別子である。プロダクトコード、Ｓ／Ｗ名も同様である。一方、クラス、有効期限開始日、有効期限終了日等はユーザ固有の情報であり、そのユーザの契約内容を反映させた情報が書き込まれる。

【００５０】以上述べてきた各情報を備えているのが管理データテーブル２であり、その論理的構成を図７に示す。

【００５１】次に、計算機本体１０のＣＰＵ－ＩＤ（筐体番号）の格納場所について説明する。本実施例においては筐体番号は、図８に示すように基本筐体内のＳＶＰとＣＥパネル間に接続されている固有筐体アドレスボード内に格納されている。また、他の方式として不揮発性記憶媒体（例えばシステムディスク）の特定エリアにあってもよい。

【００５２】次に、本実施例の資源利用方式におけるＳ／Ｗ管理について説明する。図９はＳ／Ｗ管理機能を実現する構成を示す概要図である。この図を用い、まずＳ／Ｗ管理機能の仕組みを説明する。

１）ベンダマシンからのＩＣカード作成／変更について、図９及び図１０を用いて説明する。

（１）契約内容（Ｓ１０）に従って、顧客データベースメンテナンス手段３０１を用い、顧客データベース３０３を生成／更新する（Ｓ１１）。

（２）次にＳ１２において、ＩＣカード作成手段３０２を用いて、更新された顧客データベース３０３からＩＣカードの作成／変更を行う。ＩＣカード作成手段３０２は、ＩＣカードに関するＳＶＣインタフェース３０６、カーネル３０４を用いてＩＣカードのＲＥＡＤ／ＷＲＩＴＥ等を行う。

【００５３】２）ユーザマシンでの動作について図９及び図１１を用いて説明する。

（１）ＩＰＬ時、他のイニシャライザプログラムにさきがけてＩＣカードチェック手段３０７が実行され、ＩＣカードに関して図１１に示すフローに従ってチェックを行う。ＩＣカードの内容に変更が生じた場合にはその都度チェックが必要となる。

（ａ）特権フラグが設定されているか？（Ｓ２０）

特権フラグはＩＣカード内の情報ではなくＯＳ内部に持つ情報である。このフラグを設定することにより、ＩＣカードのチェックなしで全てのソフトウェアを動作させることができる。なお、この機能は非公開とする。

（ｂ）正常なＩＣカードが装着されているか？（Ｓ２１）

ＩＣカードへのアクセスがエラーとなる場合（ＩＣカードが装着されていない場合も含む）ＳＶＰディスク３１１に格納されている以前に記憶された管理データテーブルを読み込む（Ｓ２３、Ｓ２４）。ＳＶＰディスク３１１に管理データテーブルがない場合には最低限の機能を

12

実行できる縮退モードで立ち上がる（Ｓ２３、Ｓ３３）。ＳＶＰディスクの情報から立ち上がる場合には、そのファイルの生成日が調べられ、一定期間以上経過していた場合には縮退モードで立ち上がる（Ｓ２５、Ｓ３３）。

（ｃ）ＩＣカード内の管理データテーブルの読み込み（Ｓ２２）

読み込む情報には以下のようなものがある。

読み込まれる情報：ユーザレベル、動作可能ＣＰＵ台数、ＣＰＵ－ＩＤ、ＯＳ名、ＯＳ版名（バージョン名ともいう）と有効期限、使用可能なＳ／Ｗの種類・版名・有効期限・製品クラスｅｔｃ．

（ｄ）読み込んだ管理データテーブルの正当性チェック（Ｓ２６）

ＡＤＦの持つＡＰＷ（ＡＤＦ毎のパスワード）と照合するために、セキュリティ管理プログラムは、ＩＣカードを使用してシステムを立ち上げようとするユーザにパスワードの入力を要求する。そしてセキュリティ管理プログラムは、コンソールから入力されたパスワードとＡＰＷをチェックし、異なると判定された場合には縮退モードで立ち上がる。契約期限切れの近いＳ／Ｗに関しては、ＩＰＬ時メッセージでその旨を通知する（Ｓ２７、Ｓ２８）。

（ｅ）読み込んだ管理データテーブルのメモリ上のＩＣカード情報テーブル３０５への格納（Ｓ２９）

前述した（ｄ）のチェックがＯＫであった場合、ＩＣカードから読み込んだ管理データテーブルをメモリ上のＩＣカード情報テーブル３０５へ格納する。ＩＣカード情報テーブル３０５はメモリダンプ等で解読されないよう暗号化する。また、前述した（ｂ）の次回のＩＰＬ時チェック（Ｓ２１、Ｓ２３）で使うため、ＩＣカード内の管理データテーブルをＳＶＰディスク３１１へ書き込む（Ｓ３０）。

（ｆ）ＩＰＬ回数の加算（Ｓ３１）

前述した（ｄ）で正常と判断された場合には、メモリ上のＩＣカード情報テーブル３０５のＩＰＬ回数に１加算する。

【００５４】（２）ＩＣカードチェック手段３０７の動作により正常なシステムと判断された場合通常のＩＰＬが実行され、以後各Ｓ／Ｗはその起動時以下の方法によってＯＳによる起動時チェックを受け、契約Ｓ／Ｗのみが動作する。その機能の動作時必ず実行されるモジュール（ＩＰＬ時イニシャライザ等）の動作の先頭で、ＯＳが提供するＳＶＣインタフェース３０６のチェックシステムコールを呼ぶ。それがノーマルリターンした場合以外はエラー終了させる。ＳＶＣインタフェース３０６のチェックシステムコールは、引数としてその製品のコード、版名等をもらい、ＩＣカード情報テーブル３０６と照らし合わせ、動作可／不可、製品クラス等を返す。また、起動回数をカウントしたいＳ／Ｗ製品に関しては、

13

その意志を伝える引数も渡す。これにより、ＩＰＬ後シャットダウンするまでの起動回数がメモリ上に記録され、シャットダウン時、それがＩＣカード上の管理データテーブル中の累積起動回数に加算される。

【００５５】（３）ＩＣカードの管理データテーブルをモニタする管理データテーブルモニタ機能３１０（図９参照）を提供し、ユーザレベルでどのソフトウェアが動作可能かを確認できるようにする。

【００５６】次にアプリケーションプログラムからのＳＶＣインタフェース３０６のチェックシステムコール（ｉｓｃｈｇｅｄ）について説明する。各Ｓ／Ｗは、メインとなるモジュールおよびｎ個のサブモジュールから構成されている。図１２にＳ／Ｗの関係を表すブロック図を示す。Ｓ／Ｗはメインとなるモジュールが起動された直後本システムコールを呼び出し、リターン値を受け取る。ＯＳによるＩＣカード情報テーブルとのチェックを行い、そのリターン値が正常値である場合のみ動作を続行し、エラーリターンした場合にはその旨をメッセージ出力し、アボートさせる。ここまでの処理の流れを図１３に示す。本システムコールが呼び出される箇所は、

１）イニシャライザー、ユーザから直接呼び出せるロードモジュールの先頭等、その箇所でアボートすることにより、その機能が使い物にならない箇所であること、

２）アボートしたことをユーザが気付き易い箇所であること、

３）コール回数が必要最小限であること。起動回数をカウントする必要があるものは、その値が意味のあるような箇所であること、という条件を満たさなければならない。

（１）チェックシステムコールのコーリング・シーケンスは、たとえば、以下のようなものである。

```
#include<charge.h>
int ischrged(prdctcd, version, classp, cntreq);
int prdctcd;／*製品コード*／
char *version;／*製品のバージョン*／
int *classp;／*製品クラス値へのポインタ*／
int cntreq;／*起動回数カウント要求フラグ*／
int nomsg;／*メッセージ不要フラグ*／
```

（２）チェックシステムコールの機能について説明する。ｐｒｄｃｔｃｄで指定された製品コードのｖｅｒｓｉｏｎで指定された版の製品が、そのシステムにおいて起動が許されているかどうかをチェックする（各Ｓ／Ｗにおいて自らの製品コードおよびバージョンを指定する）。製品クラスのある製品は、ｃｌａｓｓｐを指定してやり、正常リターン時に返されるクラス値に応じた動作をする。製品クラスのない製品ではＮＵＬＬを指定する。ｃｎｔｒｅｑにＮＥＥＤ＿ＣＯＵＮＴ（＝１）を指定すると、本ＳＶＣの処理の中で、その製品の起動回数が１加算される。その情報はシャットダウン時、ＩＣカード内の累積起動回数に加算される。これにより、その製品の使用頻度を知ることができる。起動回数をカウントする必要のない場合にはＮＵＬＬを指定する。ｐｒｄｃｔｃｄおよびｖｅｒｓｉｏｎで指定できる値およびｃｌａｓｓｐに返される値については、ｃｈａｒｇｅ．ｈに定義されている。通常ｉｓｃｈｒｇｅｄはエラー検出時エラーメッセージを起動端末に出力するが、これが不要な場合にはｎｏｍｓｇにＮＯＭＳＧ（＝１）を指定してやる。

14

（３）チェックシステムコールのリターン値は以下のとおりである。

起動を認められている・・・・０
起動を認められていない（非契約）・・・１
起動を認められていない（契約期間外）・・・２
エラー終了した・・・・・・－１

【００５７】次に被プロテクトノードがＨ／Ｗの場合について説明する。この実施例においては、図５に示すように、管理データテーブル内のユーザ管理情報にその計算機システムにおいてＯＳがサポートできるＨ／Ｗの制限数あるいは制御量に関する情報が記述されているものとする。ＳＶＰはまた、計算機の持っている日付が、ユーザ管理情報の中の使用開始可能日と有効期限の間であることを確認する。もし有効期限の間でなければ以降のチェックは行わない。システムの立ち上げ時に、サービスプロセッサはＨ／Ｗの制限数あるいは制御量に関する情報を参照する。また、サービスプロセッサは、その計算機に接続されている各Ｈ／Ｗの構成を独自のやりとりによって確認する機能を有している。そして、確認したＨ／Ｗの台数を記憶するレジスタを有し、そのレジスタに書き込まれた台数とユーザ管理情報内の制限数を比較し、制限数の範囲内であれば、そのＨ／Ｗを正式にこれから立ち上げる計算機のシステム構成に加えて、ＩＰＬを行う。例えば、ユーザ管理情報において制限されたワークステーション台数が３台（まで）と記述されているとき、実際に物理的に接続されているワークステーションが２台であったとき、その２台のワークステーションは論理的にも計算機に接続が許可され、使用可能となる。また、物理的に接続されているワークステーションが３台であっても、ユーザ管理情報において記述されている台数以内、すなわち３台以内であるので、同様に接続が許可され、その計算機において使用可能となる。

【００５８】次に、物理的に接続されているワークステーション台数が４台以上であった場合を説明する。この場合、最初の３台までは接続が許可されるが、４台目以降のワークステーションは物理的に線はつながっていても、計算機のシステム構成には含まれない。ここで、最初の３台というのはＳＶＰによって認識される順序によ

るので、どのワークステーションが接続不可となるのかはＳＶＰに依存している。ここではワークステーションを例にとって説明したが、台数で数えられるＨ／Ｗに関しては同様に判断される。すなわち、ＦＸＤ（固定ディスク）、データベースプロセッサ、ＭＴなどである。

【００５９】次に、被プロテクトノードが主記憶装置である場合について述べる。主記憶装置がメモリーボード単位で数えられるとき、その数によって前述したように計算機での使用を制限することができる。また他の方法として、実装されている全てのメモリーに一連のアドレスがふられているときは、使用可能なアドレス範囲情報を指定することによって、その識別カードを持つユーザに許可されている容量を使用可能とするやり方でもよい。また、この２つの方式は被プロテクトノードがキャッシュメモリで、ハード的に設定されている場合にも適用可能である。つまりキャッシュメモリに割り当てるメモリーボードを枚数で制限する方法と、キャッシュメモリ用として使用するメモリーのアドレスを指定する方法である。あるいは、キャッシュメモリがソフト的に実現されている場合には、キャッシュメモリ管理用のソフトウェアを本方式のＳ／Ｗ管理の対象としておくことによって、使用を制限することも可能である。さらにこれらの方式を組み合わせることによって、全ての整合性がとれた場合のみ、実際にキャッシュメモリを使用可能とする方法も有効である。

【００６０】次に、被プロテクトノードが計算機クロック周波数であった場合について述べる。これにはシステム立ち上げ時にパラメータを受け取ることによって、指定されたクロック周波数を発生させる手段が計算機にあらかじめ備えられていることを前提としている。計算機はＳＶＰによって管理データテーブルからユーザに許可されたクロック周波数を受け取り、そのクロック周波数で稼働する。

【００６１】以上のように、この実施例に係わるプログラムロード方式及び周辺機器インストール方式計算機は計算機筐体に設けられた個別の識別子とその計算機にオプションとして接続されるＨ／Ｗ、或はその計算機上で動作するＳ／Ｗを、識別カードおよびＳＶＰにより、カード内に記録された被プロテクトノードを記述した管理データテーブルのデータに従って認証させ、それらの接続あるいは起動を制限するものである。

【００６２】本実施例においては、認証用の識別カードは当該計算機に対し一枚しか存在せず、それぞれ対応する一台の計算機においてでしか機能しないので、識別カードの対象計算機が限定されることによって、その計算機で使用されるＳ／Ｗあるいは周辺機器の制限情報は確実に固有のものとなり、セキュリティ効果は増大する。また、識別カードを使用することより、その中へ格納する被プロテクトノードを記述した管理データテーブルのデータを不法に読取、改ざんされる危険を防止する。そしてその対象を動作するプログラムのみではなく、接続されるＨ／Ｗコンフィグレーション情報まで広げることにより、容易なモデルレパートリの拡張を実現する。またＳＶＰに識別カードとのインタフェースを設けることにより、既存の基本処理装置、各周辺機器コントローラは変更する必要はなく、容易にシステムに組入れる事ができる。更にＳＶＰを経由して遠隔地から識別カードのアクセスを可能にすることにより、被プロテクトノードを記述した管理データテーブルの読取、更新を遠隔地から行うことを可能にする。

【００６３】この実施例の利点として、以下のようなものがあげられる。

・より万全なセキュリティシステムの提供。
・必要な機能だけ購入できるＯＳ分の分割化。
・Ｓ／Ｗの試使用精度等の新しいサービスの提供。（遠隔運用保守システムと連携した場合）
・ＳＥ作業の省力化。
・ディーラＳ／Ｗの不正使用防止対策を支援。
・Ｓ／Ｗ製品の契約による売上の確保。
・保守性向上。
・出荷作業の省力化。
・ロイヤリティ支払いの適正化。
・メーカによる顧客管理の実施。

また、この実施例によれば、システムの不正使用の防止をはかることができる。また、顧客管理システムを導入することにより、ユーザ登録制度を実施し、メーカでも顧客管理ができる。

【００６４】実施例２．図１４を用いて他の実施例を説明する。図１４はこの発明におけるユーザ管理情報の別の例である。実施例１において、ワークステーションの接続台数を制限する例を説明したが、単に台数のみのチェックでなく、接続可能なモデルを制限するようにしてもよい。すなわち、モデルコードを管理データテーブルに設定しておき、ワークステーションから読み取ったモデルコードと比較して、一致した場合のみ接続を許可する方式でもよい。さらに、モデルコードを一致させたうえで台数も制限するという方式でもよい。この場合のユーザ管理情報中には前述した項目に加えて、ワークステーションのようにモデルコードを有する被プロテクトノードについては、被プロテクトノード毎に有効なモデルコードを記述する項目も設定しておく。具体的には図１４に示すように、実施例１で使用したユーザ管理情報にモデルコードに関する項目を追加する。なお、このモデルコードの設定は必要に応じて、それぞれの被プロテクトノード毎に複数設定してもよい。具体的には１項目についてモデルコードを配列のように並列的に複数書いてもよいし、ワークステーションモデルコード１、ワークステーションモデルコード２，・・・ｎのように項目を複数にしてもよい。サービスプロセッサは設定されている書式に沿って、必要な情報を読み取れるようあらかじ

め知らされているものとする。

【００６５】実施例３．次に図１５を用いて他の実施例について説明する。この図では、図７に示した管理データテーブルの構成に、さらに、接続Ｈ／Ｗ管理情報をあわせ持つ。この実施例においては、管理データテーブル中に接続Ｈ／Ｗ管理情報を持つ。前述したＳ／Ｗ管理情報と同様に、被プロテクトノードである各Ｈ／Ｗは、それぞれＨ／Ｗのカテゴリーを識別する被プロテクトノード識別子を有している。その被プロテクトノード識別子毎に１つの接続Ｈ／Ｗ管理情報を使用する。接続Ｈ／Ｗ管理情報のデータフォーマットを図１６に記す。図１６に示すように、接続Ｈ／Ｗ管理情報は図５に示したユーザ管理情報のＨ／Ｗに関する項目を別個独立に持つものである。サービスプロセッサは、その計算機に接続されている各Ｈ／Ｗの構成を独自のやりとりによって確認する機能を有しており、Ｈ／Ｗ確認時に、サービスプロセッサは、そのＨ／Ｗの被プロテクトノード識別子を受け取り、その情報をもとに、該当する接続Ｈ／Ｗ管理情報を参照する。この時、ＳＶＰはその被プロテクトノードの登録日と使用有効期限を計算機の持つシステム日付と照合し、有効でなければその被プロテクトノードの接続を許可しない。また、ＳＶＰは確認したＨ／Ｗの台数を記憶するレジスタを有し、そのレジスタに書き込まれた台数と参照した接続Ｈ／Ｗ管理情報内の最大接続台数を比較し、その制限数の範囲内であれば、そのＨ／Ｗを正式にこれから立ちあげる計算機のシステム構成に加えて、ＩＰＬを行う。具体的な判断の流れについては、実施例１と同様であるので説明を省略する。実施例１との違いは参照する情報の書かれている場所が接続Ｈ／Ｗ管理情報内であるということである。

【００６６】なお、実施例１と同様に、ワークステーションだけでなく、台数で数えられるＨ／Ｗに関しては上述した例と同様に、接続Ｈ／Ｗ管理情報を参照して、システム構成への包含の可否が判断される。すなわち、ＦＸＤ、データベースプロセッサ、ＭＴなどのシステム構成への包含の可否が判断される。

【００６７】また、主記憶装置がメモリーボード単位で数えられる時や、キャッシュメモリ用として使用するメモリボードを枚数で制限する場合もこの方式を適用できる。また、接続Ｈ／Ｗ管理情報のレイアウトを図１７のようにすれば、メモリボードの枚数でない方法で、使用許可の制限を行う場合にも適用できる。図１７（ａ）は被プロテクトノードが主記憶装置の場合である。図１７（ｂ）は被プロテクトノードがキャッシュメモリの場合である。図１７（ｃ）は被プロテクトノードが計算機クロック周波数の場合である。例えば、実装されている全てのメモリーに一連のアドレスがかかれているときは、図１７（ａ）のＬＩＭＩＴＩＮＦＯ（使用可能アドレス範囲情報）をＳＶＰが参照し、許可されているメモリ容量をその識別カードを持つユーザに対して使用可能とする。また、被プロテクトノードがキャッシュメモリであるとき、図１７（ｂ）に示すようにＬＩＭＩＴＩＮＦＯ（キャッシュメモリ割当アドレス範囲情報）をＳＶＰが参照し、指定されているアドレスの範囲をキャッシュメモリとして使用可能にする。また、被プロテクトノードが計算機クロック周波数であった場合、図１７（ｃ）に示すようなＬＩＭＩＴＩＮＦＯには使用可能周波数クロック情報が記述されており、ＳＶＰはそのユーザに許可されたクロック周波数情報を使用して、計算機をそのクロック周波数で稼働させる。この場合も実施例１と同様に、システム立ちあげ時にパラメータを受け取ることによってそのパラメータに応じてクロック周波数を可変的に設定できる手段があることを前提としている。以上のようにこの実施例においては、被プロテクトノード毎に接続Ｈ／Ｗ管理情報を識別内の管理データテーブルに持つことによって、被プロテクトノードを必要に応じて、個別に任意の使用許可条件を設定できる。

【００６８】実施例４．次に、被プロテクトノードを台数や容量でのみでなくＨ／Ｗのモデルコード毎に接続を制限する他の実施例について説明する。この実施例においては、図１８に示すように、接続Ｈ／Ｗ管理情報の中にモデルコードとそのモデルコード毎の最大接続数を記録しておく。また、前述した実施例と同様、接続Ｈ／Ｗ管理情報と計算機の持つ日付のチェックも行われるものとする。これは以降の実施例全てにおいて共通であるので以降説明を省略する。実施例１，２と同様に被プロテクトノードがワークステーションである場合を例にとる。ＳＶＰはシステム立ち上げ時に、物理的に接続されているワークステーションからモデルコードを読み取り、接続Ｈ／Ｗ管理情報中に設定されているモデルコード比較して、一致している場合のみ論理的にも接続を許可し、システム構成に加える。最初に書かれているモデルコードと一致しなければ、２番目のモデルコードと比較し、一致していれば接続を許可する。ここでも一致しなければ、３番目のモデルコードと比較する、というように、ＳＶＰは１つのワークステーションに対して一致するまですべてのエントリーとの比較を繰り返し、ｎ個目のモデルコードも不一致であった時は、そのワークステーションに対しては接続を許可しない。そして、ＳＶＰは次のワークステーションまたは他のＨ／Ｗのチェックを続行する。ワークステーション以外の他のＨ／Ｗについても、チェックの手順は同様である。モデルコードを有するＨ／Ｗであれば、この方式は適用可能である。ここでは、モデルコードのみを比較する例で説明しているが、この場合モデルコード毎の最大接続数にはＮＵＬＬが入っているものとする。

【００６９】実施例５．次に実施例４と同様に図１８に示す接続Ｈ／Ｗ管理情報を用いて、モデルコードだけでなく接続台数の制限を行う場合について説明する。この実施例においては、実施例４とは異なりモデルコード毎

の最大接続数には、実際に接続を許可する有効な数字が入っているものとする。さらにＳＶＰは被プロテクトノード毎、モデルコード毎に接続を許可されたＨ／Ｗの台数を記憶するレジスタを有しているものとする。ＳＶＰは実施例４と同じ手順で物理的に接続されているワークステーションのモデルコードと一致するモデルコードがエントリーに存在するかどうか探し、なければ論理的な接続を許可しない。もしあれば、チェック中の被プロテクトノードのモデルコードの同じ接続数が記憶されているレジスタの値を参照し、その値に１を足した数値がモデルコード毎の最大接続台数以下であるかどうかチェックする。そして、そのチェックがＯＫであれば、論理的な接続を許可する。チェックがＯＫでなければ、モデルコードが一致しても接続は許可されない。

【００７０】実施例６．また他の実施例として、前述した実施例とは異なるレイアウトを持つデータフォーマットを示す。この実施例において使用する接続Ｈ／Ｗ管理情報のデータフォーマットを図１９に示す。図に示すように、この実施例で使用する接続Ｈ／Ｗ管理情報には被プロテクトノードであるＨ／Ｗ１台毎に固有な識別子（たとえば、端末ＩＤやネットワークＩＤなど）を記述する複数の項目がある。そして個々のＨ／Ｗも１台毎に固有な識別子を記憶する手段を有しているものとする。ＳＶＰはシステム立ち上げ時にＨ／Ｗから読み取った識別子と接続Ｈ／Ｗ管理情報から読み取った識別子を比較し一致した場合のみ接続を許可する。この場合も前述した実施例同様先頭のＩＤと不一致でも、ＳＶＰは２番目、・・・ｎ番目までというように一致するまでサーチし、いずれかで一致すれば接続を許可するものとする。さらに、最大接続台数も記述しておき、識別子と二重にチェックしてもよい。

【００７１】以上のように、この実施例では、被プロテクトノードが持っている固有の識別子情報を資源利用に活用し、顧客に納入することが確定した被プロテクトノードとなるＨ／Ｗの識別子を、識別カードの管理データテーブルにあらかじめ書き込んでおくことにより、計算機の識別子との照合だけでなく被プロテクトノードの識別子の照合も行い、より厳重にチェックする方法を提供する。

【００７２】実施例７．実施例１においては、Ｓ／Ｗ管理情報の中の、Ｓ／Ｗ－ＩＤはＳ／Ｗ毎に個別だがユーザ毎、Ｓ／Ｗ毎に固有なＩＤとしてもよい。ユーザは自分用に設定された固有のＳ／Ｗ－ＩＤを持つ識別カードを使用しない限り、計算機の立ち上げ時にＳ／Ｗをロードすることができない。また、起動回数はＳ／Ｗの種類によって、実際にユーザが起動した回数を記録してもよい。さらに、ユーザが起動できる最大起動回数を保持する項目を設定し、ユーザのＳ／Ｗの起動を有効期限だけでなく累積回数で制限してもよい。

【００７３】実施例８．なお、実施例１においては、識別カードの識別子は計算機据付け時の起動で一回のみＳＶＰ７により識別カード１に書き込まれるが、必要に応じて、任意のタイミングで書き換えを行ってもよい。また、この書き換えは、例えば、公衆回線等を介して遠隔地から行ってもよい。

【００７４】実施例９．管理データテーブルの書き換えは計算機システムのオンライン稼働中も実行可能である。新たに書き換えられた管理データテーブルの情報を利用して計算機を稼働させるためには再度ＩＰＬを行えばよい。また、ＩＰＬをやり直すのではなくコマンドを使用してＩＣカード情報に従ってシステムの再構成及びＳ／Ｗのロードを行うようにしてもよい。

【００７５】実施例１０．筐体番号は導入時客先で書き込んでもよい。あるいは事前に書き込んだものを識別カードと１対にして導入してもよい。筐体番号を、出荷時には固有筐体アドレスボード内に格納せず、据付け後に書き込むことも可能である。

【００７６】実施例１１．計算機筐体に設けられた個別の識別子５を、筐体のマザーボード上のＥＥＰＲＯＭに記憶させＳＶＰ接続のコンソールにより、識別子を書換え可能としてもよい。オペレータは、パスワードにより筐体番号変更画面を開き識別番号を書換える。

【００７７】実施例１２．識別カードを、プロセッサ内蔵型ＩＣカードではなく、カード内部にセキュリティ管理プログラム３を持たないものとしてもよい。図２０において、１２はセキュリティ管理プログラム３を持たない識別カード、２は被プロテクトノードを記述した管理データテーブル、１４はセキュリティ管理プログラム、４は被プロテクトノード、５は計算機筐体に設けられた個別の識別子、１７は識別カードリーダ／ライタ、７はＳＶＰ、８は中央処理装置、９は遠隔地計算機、１０は計算機本体、１１は公衆回線、２３はインタフェース用専用Ｈ／Ｗ、２４は８ビットのデータバス、２５は１ビットの制御線である。本実施例ではＳＶＰ７内にセキュリティ管理プログラム１４を持たせ、識別カード内の管理データテーブルのセキュリティは、ＳＶＰ７とのデータ通信手順によって守られる。このとき、識別カードリーダ／ライタ１７とＳＶＰ７間をインタフェース用専用Ｈ／Ｗ２３を介し８ビットのデータバス２４と１ビットの制御線２５で結ぶ。ＳＶＰ７と識別カード１２とのデータ通信はインタフェース用専用Ｈ／Ｗ２３を通して行われる。ＳＶＰ７は識別カード１２にアクセスする時、まず識別カード１２の識別アドレス８ビットをデータ線２４を通して送る。その後規定時間後に１ビットの制御線２５にリードかライトかの情報を乗せ、データバス２４を介してデータのアクセスを行う。ＳＶＰ７では、セキュリティ管理プログラム１４によって事前に被プロテクトノード１５からの識別子を認証し整合が取れたときだけ、識別カード１２内の管理データテーブル２の情報に従い、被プロテクトノード４の起動を行う。

【００７８】この実施例は、識別カード１２にセキュリティ管理プログラムがない場合、すなわち単に管理データテーブル１３のみが存在している場合、識別カード内のデータを不正に読み取られたり不正に改ざんされたりされ易くなることを考慮したものである。すなわちＩＣカードのようにセキュリティ管理プログラムを内蔵することができる識別カードの場合には、識別カード自体がプロテクトされているのに対し、この実施例のように、識別カードが単に情報のみを記憶している場合には、この識別カードをアクセスする場合のインタフェースをメーカ独自のものとする事によりセキュリティの機能を向上させようとするものである。従って、この実施例では、標準化されたインタフェースを故意に持たず、一般には知られていない固有のインタフェースを提供する。このようにして、識別カードが単に情報を保持する場合であっても、識別カードへのアクセスを限られたシステムのみが行えるようにするものである。

【００７９】

【発明の効果】本発明は以上説明したとおり、使用される計算機ハードウエアと使用されるオプションＨ／Ｗ或は計算機ソフトウエアが一対一に限定されるためオプションＨ／Ｗ或は計算機ソフトウエアの不法な使用が防止される。また、ユーザプログラム記憶媒体には、不正防止のためのハードウエアの固有識別子を格納する必要がないので出荷形態が簡素化される。また、ユーザプログラム記憶媒体には、固有識別番号を格納する必要がないので異なったハードウエアへのインストールが自由に行える効果がある。オプションＨ／Ｗ或はソフトウエアの追加販売が識別カード内管理データテーブルの更新のみで可能になるので販売、出荷手続きが簡素化され、出荷媒体には全てのソフトウエアを格納できるので、媒体の出荷形態が簡素化される効果がある。

【００８０】また、請求項２記載の発明によれば、サービスプロセッサが識別子の照合を行うのでサービスプロセッサに変更を加えるだけで前述したような方式を容易に達成することができる。

【００８１】請求項３の記載の発明によれば、管理データテーブルを計算機側に記憶してしまうので、起動要求時の識別カードへのアクセスが不要となり、システムからカードがはずされていてもシステムに影響がなく、識別子の比較を即座に任意の時点で行うことができる。

【００８２】請求項４記載の発明によれば、ソフトウェアを起動する場合にセキュリティ管理マネージャをオペレーティングシステムに備えておくことにより、アプリケーションプログラムの起動要求に対する可否を徹底することができるので、オペレーティングシステムに対してセキュリティ管理マネージャを追加するという最小限の変更でアプリケーションプログラムの制御を行うことができる。

【００８３】さらに請求項５～１１記載の発明によれば、オプションＨ／Ｗのインストール形態が識別カードの内容により一意的に決るので、モデル毎、或は契約毎に、Ｈ／Ｗの差別化をする必要がなくなるという効果がある。

【００８４】請求項１２記載の発明によれば、計算機の識別を控え可能にしたので、計算機の製造時、出荷時、イントール時、その他任意の時点で識別子を容易に書きかえることができる。

【００８５】請求項１３記載の発明によれば、識別カードの識別子、あるいは、管理データテーブルを更新できるようにしたので、遠隔地からでも識別カードを更新することが可能になる。さらに、場合によっては、遠隔から識別カードの不法改ざんや不正使用の監視が行え、二重のチェックとなる。

【００８６】請求項１４記載の発明によれば、識別カードにプロセッサ内蔵型ＩＣカードを使用することにより管理データテーブルの不法改ざんの抑止効果を向上させる効果がある。

【００８７】また、請求項１５記載の発明によれば、識別カードにプロセッサ内蔵型ＩＣカードでなくＳＶＰとの固有なインターフェースを持つ不揮発性記憶媒体カードを使用する事によっても同様の効果を持つ。

【図面の簡単な説明】

【図１】この発明の実施例１を示すブロック図である。

【図２】この発明におけるシステム立ち上げ時チェックの流れ図である。

【図３】この発明におけるアプリケーションプログラムの起動時の流れ図である。

【図４】この発明におけるＩＣカードのメモリ構造を示す図である。

【図５】この発明におけるユーザ管理情報を示す図である。

【図６】この発明におけるソフトウェア管理情報を示す図である。

【図７】この発明における管理データテーブルの構成を示すブロック図である。

【図８】この発明のソフトウェア管理機構のハードウェア構成図である。

【図９】この発明のソフトウェア管理機能概要図である。

【図１０】この発明におけるＩＣカード作成までの手順を示す流れ図である。

【図１１】この発明におけるＩＣカードチェック手段の手順を示す流れ図である。

【図１２】この発明におけるＳ／Ｗの関係を示すブロック図である。

【図１３】この発明におけるチェックシステムコールを呼び出す流れ図である。

【図１４】この発明におけるユーザ管理情報を示す図である。

23

【図１５】この発明における管理データテーブルの構成を示すブロック図である。

【図１６】この発明における接続Ｈ／Ｗ管理情報の一例を示す図である。

【図１７】この発明における接続Ｈ／Ｗ管理情報の一例を示す図である。

【図１８】この発明における接続Ｈ／Ｗ管理情報の一例を示す図である。

【図１９】この発明における接続Ｈ／Ｗ管理情報の一例を示す図である。

【図２０】この発明の実施例１２を示すブロック図である。

【符号の説明】

１　識別カード

２　管理データテーブル

24

３　セキュリティ管理プログラム

４　被プロテクトノード

５　計算機筐体に設けられた個別の識別番号

６　識別カードリーダ／ライタ

７　ＳＶＰ

８　中央処理装置

９　遠隔地計算機

１０　計算機本体

１１　公衆回線

１２　識別カード

１４　セキュリティ管理プログラム

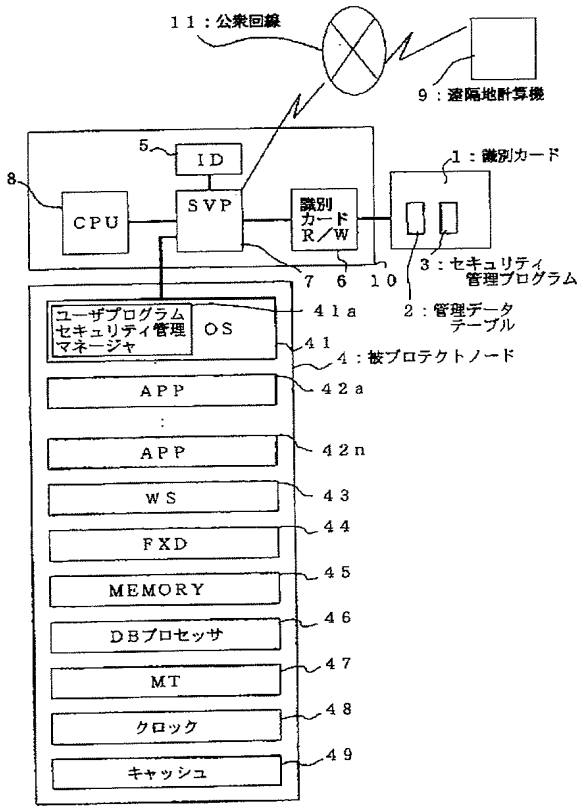
１７　識別カードリーダ／ライタ

２３　インタフェース用専用Ｈ／Ｗ

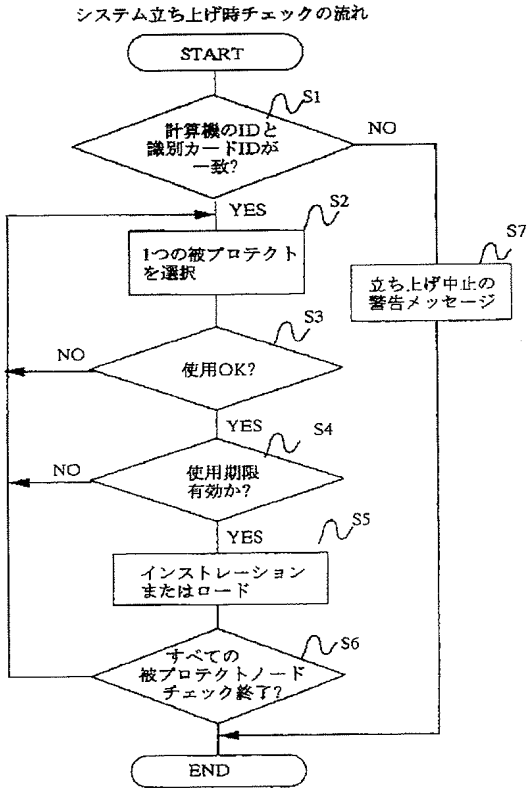
２４　８ビットデータバス

２５　１ビット制御線

【図１】



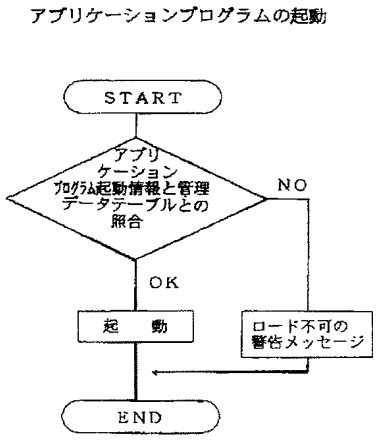
【図２】



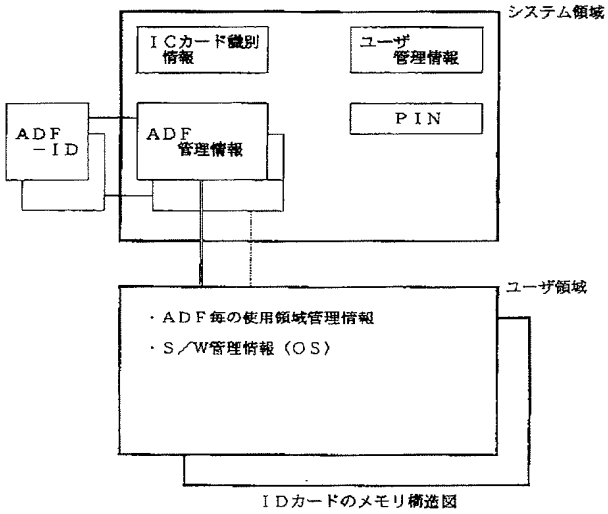
【図１６】

H／W－ＩＤ	H／Wのカテゴリー毎のＩＤ番号（被ﾌﾟﾛﾃｸﾄﾉｰﾄﾞ識別子）
STARTDAY	H／Wのカテゴリー毎の登録日
LIMITDAY	H／Wのカテゴリー毎の使用有効期限
LIMITNUM	最大接続台数

【図３】



【図４】



ＩＤカードのメモリ構造図

【図５】

ユーザ管理情報

100

	名称	説明
30	ディーラＩＤ	ディーラ識別ＩＤ
31	ユーザＩＤ	ユーザ識別ＩＤ
32	マシンＩＤ	機種／モデル識別ＩＤ
33	ユーザレベル	システム使用者識別レベル
34	使用開始可能日	ＩＣカードの使用開始可能日
35	有効期限	ＩＣカードの使用有効期限
36	更新日	ＩＣカード内データの最終更新日
37	ディーラ名	ユーザレベルに対応するディーラ名
38	ユーザ名	システム使用者名
39	マシン名	機種／モデル名
40	ＣＰＵ　ＩＤ	ＣＰＵ　ＩＤ
41	ＯＳ名	ＯＳ名
42	ＯＳ バージョン名	ＯＳ バージョン名
43	ワークステーション台数	ＯＳのサポートワークステーション台数
44	接続FXD台数	ＯＳのサポートＦＸＤ台数
45	主記憶装置容量	ＯＳのサポート主記憶装置容量
46	接続データベースプロセッサ台数	ＯＳのサポートデータベースプロセッサ台数
47	接続ＭＴ台数	ＯＳのサポートＭＴ台数
48	計算機クロック周波数	その計算機で使用するクロック周波数
49	キャッシュメモリ設定情報	キャッシュメモリとして設定するメモリ容量
50	ＩＰＬ回数	ＩＰＬ回数

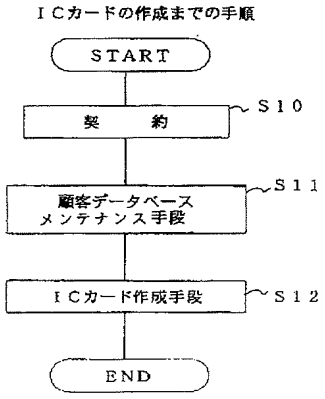
【図６】

Ｓ／Ｗ管理情報

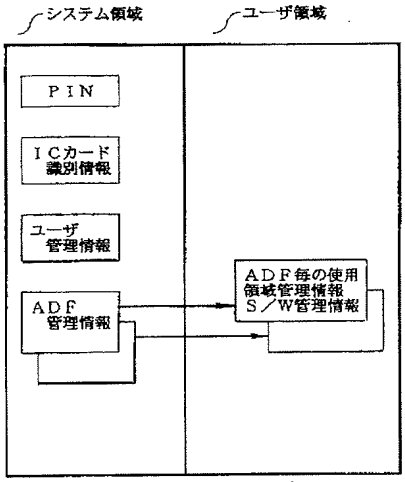
200

	名称	説明
201	Ｓ／Ｗ　ＩＤ	ソフトウェア毎の識別ＩＤ
	プロダクトコード	ソフトウェア毎の製品コード
202	Ｓ／Ｗ名	ソフトウェア毎の名称
203	クラス	製品クラス番号（Ｓ／Ｗごとのサポート・クライアント種別）が入る。クラス番号が無い場合は、ＮＵＬＬとする。
204	有効期限開始日	Ｓ／Ｗ毎の登録日
205	有効期限終了日	Ｓ／Ｗ毎の使用有効期限
206	カウント要求フラグ	起動回数カウント要求フラグ（ＯＮ：１，ＯＦＦ：０）
207	起動回数	Ｓ／Ｗ毎の起動回数
208	バージョン	Ｓ／Ｗバージョン名
209	使用フラグ	使用不可フラグ（０以外で使用可能）
210	サポートフラグ	サポートフラグ（ＯＮ：１，ＯＦＦ：０）
211	リリース	Ｓ／Ｗ毎のリリース・バージョン（無い場合はＮＵＬＬ）
212	メンテナンスフラグ	保守フラグ

【図１０】

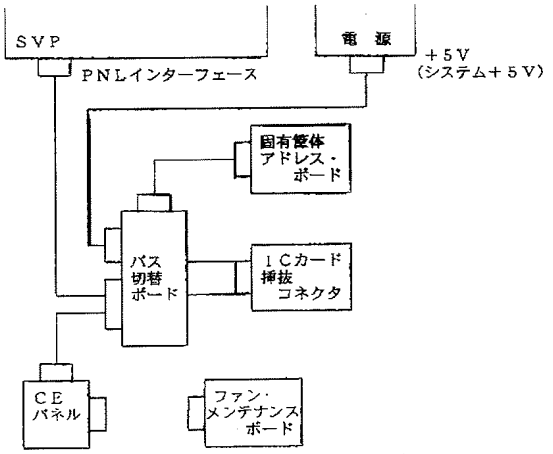


【図７】



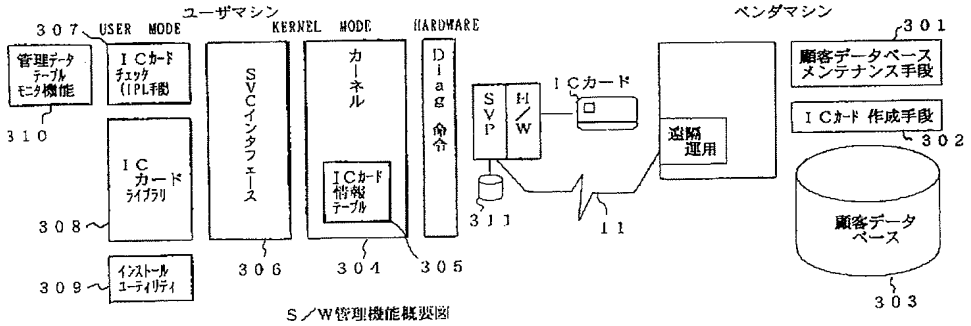
管理データテーブルの構成を示すブロック図

【図８】



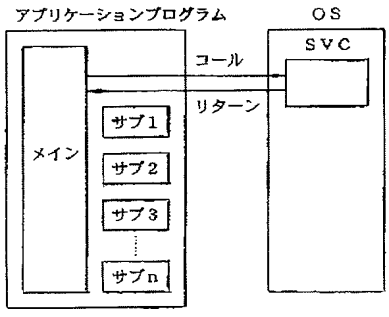
Ｓ／Ｗ管理機構のＨ／Ｗ構成図

【図９】

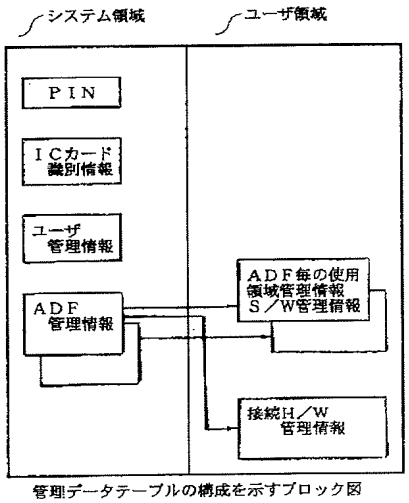


Ｓ／Ｗ管理機能概要図

【図１２】

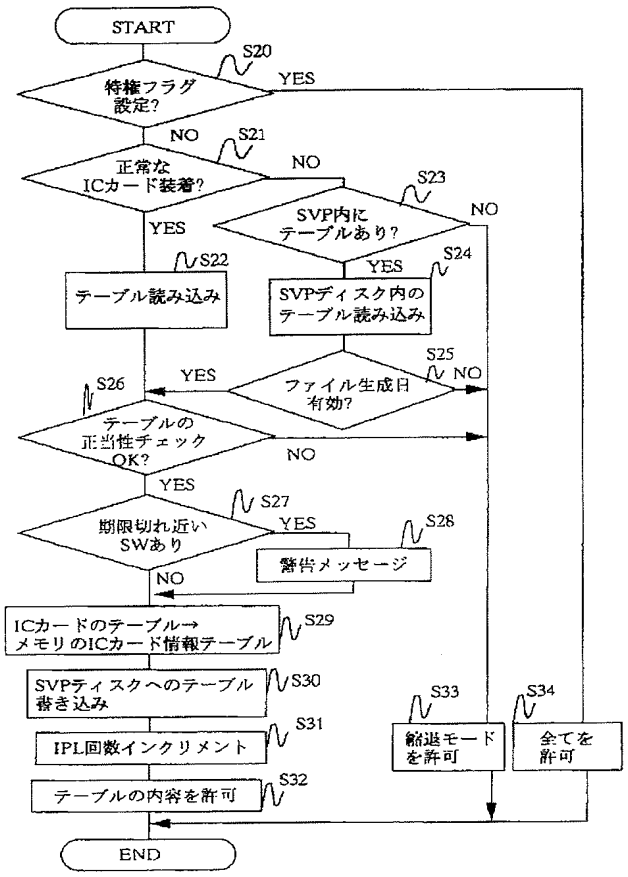


【図１５】

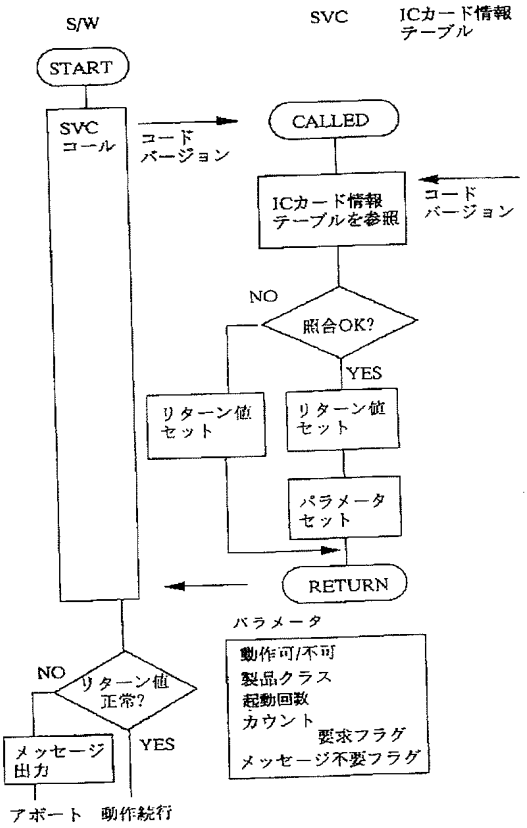


管理データテーブルの構成を示すブロック図

【図１１】



【図１３】



【図１７】

(a)

H／W－ＩＤ	H／Wのカテゴリー毎のＩＤ番号（被ﾌﾟﾛﾃｸﾄﾉｰﾄﾞ識別子）
STARTDAY	H／Wのカテゴリー毎の登録日
LIMITDAY	H／Wのカテゴリー毎の使用有効期限
LIMITINFO	使用可能メモリアドレス範囲情報

(b)

H／W－ＩＤ	H／Wのカテゴリー毎のＩＤ番号（被ﾌﾟﾛﾃｸﾄﾉｰﾄﾞ識別子）
STARTDAY	H／Wのカテゴリー毎の登録日
LIMITDAY	H／Wのカテゴリー毎の使用有効期限
LIMITINFO	キャッシュメモリ割当アドレス範囲情報

(c)

H／W－ＩＤ	H／Wのカテゴリー毎のＩＤ番号（被ﾌﾟﾛﾃｸﾄﾉｰﾄﾞ識別子）
STARTDAY	H／Wのカテゴリー毎の登録日
LIMITDAY	H／Wのカテゴリー毎の使用有効期限
LIMITINFO	使用可能クロック周波数情報

【図１８】

H／W－ＩＤ	H／Wのカテゴリー毎のＩＤ番号（被ﾌﾟﾛﾃｸﾄﾉｰﾄﾞ識別子）
STARTDAY	H／Wのカテゴリー毎の登録日
LIMITDAY	H／Wのカテゴリー毎の使用有効期限
MODELCODE 1	モデルコード
LIMITNUM 1	最大接続台数（上記モデルコードのみを対象）
MODELCODE 2	モデルコード
LIMITNUM 2	最大接続台数（上記モデルコードのみを対象）
⋮	
MODELCODE n	モデルコード
LIMITNUM n	最大接続台数（上記モデルコードのみを対象）

【図１４】

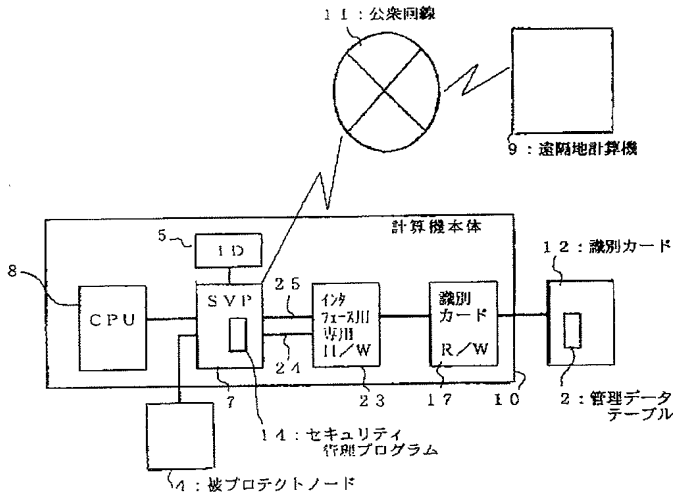
ユーザ管理情報　１００

	名称	説明
30	ディーラＩＤ	ディーラ識別ＩＤ
31	ユーザＩＤ	ユーザ識別ＩＤ
32	マシンＩＤ	機種／モデル識別ＩＤ
33	ユーザレベル	システム使用者識別レベル
34	使用開始可能日	ＩＣカードの使用開始可能日
35	有効期限	ＩＣカードの使用有効期限
36	更新日	ＩＣカード内データの最終更新日
37	ディーラ名	ユーザレベルに対応するディーラ名
38	ユーザ名	システム使用者名
39	マシン名	機種／モデル名
40	ＣＰＵ　ＩＤ	ＣＰＵ　ＩＤ
41	ＯＳ名	ＯＳ名
42	ＯＳ バージョン名	ＯＳ　バージョン名
43	ワークステーション台数	ＯＳのサポートワークステーション台数
44	接続ＦＸＤ台数	ＯＳのサポートＦＸＤ台数
45	主記憶装置容量	ＯＳのサポート主記憶装置容量
46	接続データベースプロセッサ台数	ＯＳのサポートデータベースプロセッサ台数
47	接続ＭＴ台数	ＯＳのサポートＭＴ台数
48	計算機クロック周波数	その計算機で使用するクロック周波数
49	キャッシュメモリ設定情報	キャッシュメモリとして設定するメモリ容量
50	ＩＰＬ回数	ＩＰＬ回数
	ワークステーションモデルコード	
	ＦＸＤモデルコード	
	データベースプロセッサモデルコード	
	ＭＴモデルコード	

【図１９】

Ｈ／Ｗ－ＩＤ	Ｈ／Ｗのカテゴリー毎のＩＤ番号（被プロテクトノード識別子）
STARTDAY	Ｈ／Ｗのカテゴリー毎の登録日
LIMITDAY	Ｈ／Ｗのカテゴリー毎の使用有効期限
ＩＤ　１	Ｈ／Ｗ１台毎に固有な識別子
ＩＤ　２	Ｈ／Ｗ１台毎に固有な識別子
⋮	
ＩＤ　ｎ	Ｈ／Ｗ１台毎に固有な識別子
LIMITNUM	最大接続台数

【図２０】



(19)日本国特許庁（ＪＰ）　(12)**公表特許公報**（Ａ）　(11)特許出願公表番号
特表2002－518720
（P2002－518720A）
(43)公表日　平成14年６月25日(2002.6.25)

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｄ　５Ｂ０８５

審査請求　未請求　予備審査請求　有　（全 66 頁）

(21)出願番号　特願2000－554109(P2000－554109)
(86)(22)出願日　平成11年６月９日(1999.6.9)
(85)翻訳文提出日　平成12年12月12日(2000.12.12)
(86)国際出願番号　ＰＣＴ／ＵＳ９９／１２９１３
(87)国際公開番号　ＷＯ９９／６５２０７
(87)国際公開日　平成11年12月16日(1999.12.16)
(31)優先権主張番号　０９／０９６，６７６
(32)優先日　平成10年６月12日(1998.6.12)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＪＰ

(71)出願人　マイクロソフト　コーポレイション
ＭＩＣＲＯＳＯＦＴ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国　ワシントン州　98052－6399　レッドモンド　ワン　マイクロソフト　ウェイ　（番地なし）
(72)発明者　マリオ　シー．　ゴートゼル
アメリカ合衆国　98033　ワシントン州　カークランド　ノースイースト　107　プレイス　12631
(74)代理人　弁理士　谷　義一　（外２名）

最終頁に続く

(54)【発明の名称】　セキュリティ・ロケーション識別の方法およびシステム

(57)【要約】
ネットワーク・リソースへのアクセスが接続しているユーザーのロケーションを含む情報に基づいている改善されたコンピュータ・ネットワーク・セキュリティ・システムおよび方法である。一般に、ユーザーのロケーションの信頼性が低い場合、そのユーザーに割り当てられるアクセス権はより制限される。識別機構およびプロセスは、ローカル・ユーザー、イントラネット・ユーザおよびダイアルアップ・ユーザーなどを互いに区別するなど、セキュリティ方針のカテゴリに関してユーザーのロケーションを決定する。ロケーションおよびユーザーの資格認定を含む情報に基づいて、ユーザーの通常のアクセス・トークン内のユーザーに基づいたセキュリティ情報を越えてユーザーのプロセスを制限せず、一方、ダイアルアップ接続を介して接続しているときには同じユーザーのリソースへのアクセスをさらに制限するなどの、セキュリティ方針に従って、ユーザーの通常のアクセスを制限できるアクセス・トークンが設定される。制限付きトークンは、好ましくは、信頼性がより低いロケーションから接続しているユーザーのセキュリティ・コンテキストを制限することによる前記ロケーションに基づいた識別を実装するために使用される。

【特許請求の範囲】

【請求項１】　ユーザーが複数の仮想的なロケーションのうち１つのロケーションからネットワークに選択的に接続することができるコンピュータ・ネットワークにおいて、改善されたネットワーク・セキュリティを提供する方法であって、

前記ユーザーが接続しているロケーションを決定するステップと、

前記仮想的なロケーションを含む基準に基づいて少なくとも２つの異なるアクセス・レベルから前記ユーザーのアクセス・レベルを選択するステップと、

前記ユーザーを前記ネットワークに接続するステップと、

前記アクセス・レベルを含む情報に基づいて、ネットワーク・リソースへの前記ユーザーのアクセスを決定するステップ

とを備えることを特徴とする方法。

【請求項２】　前記ユーザーにインターネット・プロトコル・アドレスを割り当てるステップであって、前記割り当てられるアドレスはユーザーが接続しているロケーションによって決めるステップをさらに備えることを特徴とする請求項１に記載の方法。

【請求項３】　前記ユーザーが接続しているロケーションを決定するステップは、前記ユーザーに割り当てられたインターネット・プロトコル・アドレスを査定するステップを備えることを特徴とする請求項１に記載の方法。

【請求項４】　前記少なくとも２つの異なるアクセス・レベルからアクセス・レベルを選択するステップは、前記インターネット・プロトコル・アドレスに従って前記アクセス・レベルを選択するステップを備えることを特徴とする請求項３に記載の方法。

【請求項５】　前記ユーザーが接続しているロケーションを決定するステップは、前記ユーザーがリモート・アクセス・サーバを介して前記ネットワークに接続していることを決定するステップを備えることを特徴とする請求項１に記載の方法。

【請求項６】　前記ユーザーがダイアルアップ接続を介して接続しているかどうかを決定するステップをさらに備えることを特徴とする請求項５に記載の方

法。

【請求項７】　前記ユーザーがダイアルアップ接続を介して接続していると決定され、さらに、前記ユーザーが接続している電話番号を決定するステップと、前記電話番号を登録済みユーザーのリストと比較するステップとを含み、前記アクセス・レベルを選択するステップは、前記電話番号が前記リスト内にある場合には１つのレベルを選択し、前記番号が前記リストにない場合には別のレベルを選択するステップを備えることを特徴とする請求項６に記載の方法。

【請求項８】　前記ユーザーが接続しているロケーションを決定するステップは、前記ユーザーがリモート・アクセス・サーバを介して前記ネットワークに接続しているかどうかを決定するステップを備え、前記ユーザーがリモート・アクセス・サーバを介して接続している場合に、前記アクセス・レベルを選択するステップが、より多くの制限付きアクセス権に対応するアクセス・レベルを選択するステップを備えることを特徴とする請求項１に記載の方法。

【請求項９】　前記ユーザーが接続しているロケーションを決定するステップは、前記ユーザーがイントラネットを介して前記ネットワークに接続していることを決定するステップを備えることを特徴とする請求項１に記載の方法。

【請求項１０】　前記ユーザーが接続しているロケーションを決定するステップは、前記ユーザーが仮想的な組織内ネットワークを介して前記ネットワークに接続していることを決定するステップを備えることを特徴とする請求項１に記載の方法。

【請求項１１】　情報に基づいてネットワーク・リソースへのアクセスを決定するステップは、前記ユーザーの資格認定に基づいてアクセスを決定するステップを含むことを特徴とする請求項１に記載の方法。

【請求項１２】　ネットワーク・リソースへのアクセスを決定するステップは、前記ユーザー用のアクセス・トークンを作成するステップを含むことを特徴とする請求項１１に記載の方法。

【請求項１３】　前記アクセス・トークンが前記ユーザーの各プロセスと関連付けられ、前記ネットワーク・リソースへのアクセスを決定するステップは、前記アクセス・トークン内の情報を各ネットワーク・リソースに関連付けられた

セキュリティ情報と比較するステップを含むことを特徴とする請求項１２に記載の方法。

【請求項１４】　前記アクセス・トークンを作成するステップは、前記ユーザーの通常のトークンから制限付きトークンを作成するステップと、前記制限付きトークンから前記親トークンに関連する少なくとも１つの特権を削除するステップとを含むことを特徴とする請求項１２に記載の方法。

【請求項１５】　アクセス・トークンを作成するステップは、前記ユーザーの通常のトークンから制限付きトークンを作成するステップと、前記通常のトークン内の対応するセキュリティ識別子の属性情報に関連した、前記制限付きトークン内のセキュリティ識別子の属性情報を、そのセキュリティ識別子を介したアクセスのみを拒否するために使用するように変更するステップとを含むことを特徴とする請求項１２に記載の方法。

【請求項１６】　前記ネットワークへ前記ユーザーを接続するステップは、前記ユーザーを、質疑応答型プロトコルを介して認証するステップを含むことを特徴とする請求項１２に記載の方法。

【請求項１７】　前記ユーザーを前記ネットワークへ接続するステップが、チケット発行機能によって発行されたチケットを前記ユーザーから受け取るステップを含むことを特徴とする請求項１２に記載の方法。

【請求項１８】　前記ユーザーを前記ネットワークへ接続するステップが、認証機関によって発行された前記証明を前記ユーザーから受け取るステップを含むことを特徴とする請求項１２に記載の方法。

【請求項１９】　アクセス・トークンを作成するステップは、前記ユーザーの通常のトークンから制限付きトークンを作成するステップと、少なくとも１つの制限付きセキュリティ識別子を前記制限付きトークンに追加するステップとを含むことを特徴とする請求項１２に記載の方法。

【請求項２０】　ネットワーク・リソースへのアクセスを決定するステップは、前記アクセス・トークン内のユーザー情報および少なくとも１つの制限付きセキュリティ識別子を、各ネットワーク・リソースに関連付けられたセキュリティ情報と比較するステップを含むことを特徴とする請求項１２に記載の方法。

【請求項２１】　ユーザーが複数の仮想的なロケーションのうち１つからネットワークへ選択的に接続することができるコンピュータ・ネットワークにおいて、改善されたネットワーク・セキュリティを提供するためのシステムであって、

ユーザーが接続する仮想的なロケーションを決定し、それに基づいて少なくとも２つの異なるアクセス・レベルから１つのアクセス・レベルを選択する識別機構と、

前記アクセス・レベルを含む情報に基づいて前記ユーザーのアクセス権を設定するセキュリティ・プロバイダと、

前記設定されたアクセス権に従ってネットワーク・リソースへのユーザー・アクセスを決定する実施機構

とを備えることを特徴とするシステム。

【請求項２２】　前記識別機構は、それによって決定された前記仮想的なロケーションに基づいて前記ユーザーにインターネット・プロトコル・アドレスを割り当てることを特徴とする請求項２１に記載のシステム。

【請求項２３】　前記識別機構は、前記ユーザーに割り当てられたインターネット・プロトコル・アドレスを査定することを特徴とする請求項２１に記載のシステム。

【請求項２４】　前記識別機構は、前記インターネット・プロトコル・アドレスに従って前記アクセス・レベルを選択することを特徴とする請求項２３に記載のシステム。

【請求項２５】　前記識別機構は、前記ユーザーがリモート・アクセス・サーバを介して前記ネットワークに接続していることを決定することを特徴とする請求項２１に記載のシステム。

【請求項２６】　前記識別機構は、さらに、前記ユーザーがダイアルアップ接続を介して接続していることを決定することを特徴とする請求項２５に記載のシステム。

【請求項２７】　登録済み電話番号のリストおよび前記識別機構に接続された発呼者ＩＤ機構をさらに備え、前記識別機構は発呼者ＩＤ機構にアクセスして

前記ユーザーの電話番号を決定し、前記リストにアクセスして前記電話番号が前記リスト内にあるかどうかを決定し、前記電話番号が前記リスト内にある場合は１つのアクセス・レベルを決定し、前記番号が前記リスト内にない場合に別のアクセス・レベルを決定することを特徴とする請求項２６に記載のシステム。

【請求項２８】　前記識別機構は、前記ユーザーがリモート・アクセス・サーバを介して前記ネットワークに接続しているかどうかを決定し、前記ユーザーがリモート・アクセス・サーバを介して接続している場合、さらに、前記ネットワークへの直接接続に対して選択される前記ユーザーのアクセス権に比較してより制限されたアクセス権に相当するアクセス・レベルを前記ユーザーに対して選択することを特徴とする請求項２１に記載のシステム。

【請求項２９】　前記識別機構は、前記ユーザーがイントラネットを介して前記ネットワークに接続している時日を決定するための手段を含むことを特徴とする請求項２１に記載のシステム。

【請求項３０】　前記識別機構は、前記ユーザーが仮想的な組織内ネットワークを介して前記ネットワークに接続している時を決定するための手段を含むことを特徴とする請求項２１に記載のシステム。

【請求項３１】　前記セキュリティ・プロバイダは、前記ユーザーの前記資格認定を含む情報に基づいて前記ユーザーのアクセス権を設定することを特徴とする請求項２１に記載のシステム。

【請求項３２】　前記セキュリティ・プロバイダは前記ユーザー用のアクセス・トークンを作成することを特徴とする請求項２１に記載のシステム。

【請求項３３】　前記アクセス・トークンは、前記ユーザーの各プロセスに関連付けられ、前記実施機構が前記アクセス・トークン内の情報を各ネットワーク・リソースに関連付けられたセキュリティ情報と比較することによって、前記ネットワーク・リソースへのアクセスを決定することを特徴とする請求項３２に記載のシステム。

【請求項３４】　ファイルをその上に有するコンピュータ・サーバ内において、前記ファイルへのアクセスを選択的に制限する方法であって、

要求をエンティティから受け取ってファイルへアクセスするステップと、

前記エンティティのタイプを含む基準に基づいて少なくとも２つの異なるアクセス・レベルから前記エンティティ用のアクセス・レベルを選択するステップと、

前記アクセス・レベルを含む情報に基づいて、前記エンティティの前記ファイルへのアクセスを決定するステップ

とを含むことを特徴とする方法。

【請求項３５】　前記エンティティは、リモート・コンピュータ・システムのプロセスであって、前記少なくとも２つの異なるアクセス・レベルから前記エンティティ用のアクセス・レベルを選択する前記ステップは、前記ローカル・サーバのプロセスに対しては第１のアクセス・レベルを割り当て、前記リモート・コンピュータのプロセスに対しては第２のアクセス・レベルを割り当てるステップを含むことを特徴とする請求項３４に記載の方法。

【請求項３６】　前記エンティティは、前記コンピュータ・サーバ上で実行しているスクリプトであり、前記少なくとも２つの異なるアクセス・レベルから前記エンティティ用のアクセス・レベルを選択するステップは、スクリプトに対して異なるアクセス・レベルを割り当てるステップを含むことを特徴とする請求項３４に記載の方法。

【請求項３７】　前記エンティティは、前記コンピュータ・サーバ上で稼働しているＦＴＰサーバであり、前記少なくとも２つの異なるアクセス・レベルから前記エンティティ用のアクセス・レベルを選択するステップは、ＦＴＰサーバに対して異なるアクセス・レベルを割り当てるステップを含むことを特徴とする請求項３４に記載の方法。

【請求項３８】　前記エンティティは、プロキシのプロセスであり、前記少なくとも２つの異なるアクセス・レベルから前記エンティティ用のアクセス・レベルを選択するステップは、前記ローカル・サーバのプロセス用に第１のアクセス・レベルを割り当て、プロキシのプロセス用に第２のアクセス・レベルを割り当てるステップを含むことを特徴とする請求項３４に記載の方法。

【発明の詳細な説明】

【０００１】

（発明の分野）

本発明は、一般にコンピュータ・システムに関し、より詳細には、コンピュータ・システムの改善されたセキュリティ・モデルに関する。

【０００２】

（発明の背景）

現在のコンピュータ・セキュリティ・システムは、ユーザーの資格認定（credentials）に従って与えられた許可に基づいて、ネットワーク・リソースへのユーザーのアクセスを決定する。このユーザー中心のモデルは、増大するモバイル／リモート（mobile/remote）ユーザー人口に大きな融通性を提供する。たとえば、リモート・アクセス・サーバおよびインターネットの接続性は、ユーザーが仮想的に任意のロケーションから会社のリソースにユーザーに意識させないで（transparently）アクセスすることを可能にする。

【０００３】

この融通性はユーザーおよびネットワーク所有者（たとえば会社、企業）の両方に利点を提供するが、このような増大した有用性および簡単な接続性は本質的に、許可されないアクセスについてのリスクを引き上げる。暗号化されたネットワーク通信は有線盗聴を防ぐが、機密情報のある企業リソースへのリモート・アクセスを許すという本質的なリスクを依然として有している。実際には、リソース（ファイルなど）が送信されるときに保護されているにもかかわらず、正式に認可されたユーザーが適正な任意のロケーションからアクセスされることを会社が望まない企業リソースの機密情報を含むサブセットがある可能性が依然としてある。

【０００４】

たとえば、ラップトップ・コンピュータのユーザーが飛行機の上で作業をしているときなどに、非常に機密性のある会社の戦略を意図しない閲覧者に不注意に表示する場合がある。新しい、広い視野角のラップトップ画面では、他の乗客がモニタの内容をのぞき見することを防ぐことはさらに困難である。同様に、モバ

イル・ユーザーの人口は増大しているので、ノートブック・コンピュータの盗難または紛失はさらに、機密性のある企業データのセキュリティを脅かしている。ユーザーのアカウントおよびパスワードも、特に盗まれたラップトップ上に維持されている場合は、盗まれる可能性がある。ユーザーが適切な資格認定を有する限り、既存のセキュリティ機構（security mechanism）は、リモートからファイルをダウンロードし、他のリモート・アクションを実行することが容易とし、したがって、これらのセキュリティ・リスクおよび他のセキュリティ・リスクに寄与する。

【０００５】

簡単に言えば、リモート・アクセス・サーバ（ＲＡＳ）およびインターネットの接続性は、ユーザーが仮想的な任意のロケーションから企業リソースにアクセスできるようにする。しかし、一定のロケーション（特にリモート・ロケーション）は他よりも安全ではない。たとえば、軽便でアクセスが増大されているため、ラップトップ・コンピュータへダウンロードされたファイルは、会社のオフィス内にあるデスクトップ・マシン上のファイルより簡単に盗める。同様に、許可されない人がユーザーのアカウントおよびパスワードを得る可能性もあり、これによって、彼らがリモート・ロケーションから会社のリソースへアクセスしようとする可能性が最大になる。

【０００６】

（発明の概要）

簡単に言えば、本発明は、ネットワーク・リソースへのアクセスが接続しているユーザーのロケーションを含む情報に基づいている改善されたコンピュータ・ネットワーク・セキュリティ・システムおよび方法を提供する。通常は、ユーザーのロケーションの信頼性がより低ければ、そのユーザーに割り当てられたアクセス権はより制限される。識別機構（discrimination mechanism）は、ローカル・ユーザー、イントラネット・ユーザ、およびダイアルアップ・ユーザーを互いに区別するなど、いくつかのカテゴリのセキュリティ方針に関してユーザーのロケーションを決定する。セキュリティ・プロバイダは、ロケーションおよびユーザーの資格認定を含む情報に基づいて、そのユーザー用アクセス・トークンを設

定するなどによって、そのユーザーのアクセス権を確立する。実施機構（enforcement mechanism）は、そのユーザーのために設定されたアクセス権を使用して、リソースへのアクセスを許可または拒否するかどうかを決定する。ロケーションに基づいたアクセス権は、セキュリティ方針に従って、ユーザーの通常のアクセス権に関して制限することができる。たとえば、ローカル・ユーザーのプロセスは、ユーザーの通常のアクセス・トークン内のユーザーに基づいたセキュリティ情報を越えて制限することはできないが、一方、ダイアルアップ接続を介しての同じユーザーの接続は制限付きプロセスを有する場合がある。好ましい制限付きトークンを使用して、信頼性の低いロケーションから接続しているユーザーのアクセスを制限することによって、ロケーションに基づいた識別を実行する。制限付きトークンが使用され、信頼性の低いロケーションからのユーザー接続でのアクセスを制限するによるロケーション・ベースの識別を実行することは、望ましいことである。

【０００７】

他の目的および利点は、図面を参照してなされる次の詳細な説明から明らかになろう。

【０００８】

（詳細な説明）

例としての動作環境

図１および以下の考察は、本発明が実現できる適切なコンピューティング環境の簡単で一般的な説明を提供すること、を意図している。必要ではないが、本発明は、パーソナル・コンピュータによって実行されるプログラム・モジュールなどのコンピュータ実行可能な命令の一般的なコンテキスト内で説明される。一般に、プログラム・モジュールは、ルーチン、プログラム、オブジェクト、構成要素、データ構造、そして特定のタスクを実行するか、特定の抽象的なデータ・タイプに道具を提供するもの実現するなどを含む。さらに、当業者であれば、本発明は、ハンド・ヘルド・デバイス、マルチプロセッサ・システム、マイクロプロセッサ・ベースのプログラミング可能な消費者用電気製品、ネットワークＰＣ、ミニ・コンピュータ、メインフレーム・コンピュータなどを含むほかのコンピュ

ータ・システム構成でも実行できることが理解されるであろう。本発明はまた、通信ネットワークを介してリンクされたリモート処理デバイスによってタスクが実行される分散コンピューティング環境内でも実行できる。分散コンピューティング環境では、プログラム・モジュールはローカル・メモリ記憶デバイスおよびリモート・メモリ記憶デバイスの両方に配置される場合がある。

【０００９】

図１を参照すると、本発明を実現するための１例としてのシステムは、従来のパーソナル・コンピュータ２０などの形の汎用コンピューティング・デバイスを含み、汎用コンピューティング・デバイスは、処理ユニット２１、システム・メモリ２２、および処理ユニット（processing unit）２１のためのシステム・メモリを含む種々のシステム構成要素を結合するシステム・バス２３を含む。システム・バス２３は、メモリ・バスまたはメモリ・コントローラ、周辺バス、種々のバス・アーキテクチャのうち任意のアーキテクチャを使用するローカル・バスを含むいくつかのタイプのバス構成のどれでも含むことができる。システム・メモリは、読み取り専用メモリ（ＲＯＭ）２４およびランダム・アクセス・メモリ（ＲＡＭ）２５を含む。基本入出力システム２６（ＢＩＯＳ）は、ＲＯＭ２４内に格納され、起動時などにパーソナル・コンピュータ２０内の構成要素の間で情報を転送するのに役立つ基本的なルーチンを含んでいる。パーソナル・コンピュータ２０はさらに、図示されてはいないがハードディスクから読み出したり書き込んだりするためのハードディスク・ドライブ２７、取り外し可能な（removable）磁気ディスク２９から読み出したり書き込んだりするための磁気ディスク・ドライブ２８、および、ＣＤ－ＲＯＭまたは他の光媒体など、取り外し可能な光ディスク３１から読み出したり書き込んだりするための光ディスク・ドライブ３０を含む場合がある。ハードディスク・ドライブ２７、磁気ディスク・ドライブ２８、および光ディスク・ドライブ３０はそれぞれ、ハードディスク・ドライブ・インタフェース３２、磁気ディスク・ドライブ・インタフェース３３、および光ドライブ・インターフェース３４によってそれぞれシステム・バス２３に接続されている。ドライブとその関連付けられたコンピュータ読み取り可能媒体は、パーソナル・コンピュータ２０のためにコンピュータ読み取り可能命令、データ

構造、プログラム・モジュールおよびほかのデータの、不揮発性のストレージを提供する。ここに説明された例としての環境は、ハードディスク、取り外し可能磁気ディスク２９および取り外し可能光ディスク３１を使用しているが、当業者であれば磁気カセット、フラッシュメモリ・カード、ディジタル・ビデオ・ディスク、ベルヌーイ・カートリッジ、ランダム・アクセス・メモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）などの、コンピュータによってアクセス可能なデータを格納できる他のタイプのコンピュータ読み取り可能な媒体も例としての動作環境内で使用できることが理解されるであろう。

【００１０】

オペレーティング・システム３５（好ましくはＷｉｎｄｏｗｓ　ＮＴ）、１つまたは複数のアプリケーション・プログラム３６、ほかのプログラム・モジュール３７およびプログラム・データ３８を含むいくつかのプログラム・モジュールがハードディスク、磁気ディスク２９、光ディスク３１、ＲＯＭ２４またはＲＡＭ２５に格納できる。ユーザーは、キーボード４０およびポインティング・デバイス４２などの入力デバイスを介してパーソナル・コンピュータ２０にコマンドおよび情報を入力できる。他の入力デバイス（図示せず）は、マイクロフォン、ジョイスティック、ゲーム・パッド、サテライト・ディッシュ（satellite dish）、スキャナなどを含むことができる。これらおよび他の入力デバイスはしばしば、システム・バスに結合されたシリアルポート・インタフェース４６を介して処理ユニット２１に接続されているが、パラレル・ポート、ゲーム・ポートまたは汎用シリアルバス（ＵＳＢ）などの他のインターフェースによって接続されている場合もある。モニタ４７または他のタイプの表示デバイスもまた、ビデオ・アダプタ４８などのインターフェースを介してシステム・バス２３に接続されている。モニタ４７の外に、パーソナル・コンピュータは典型的にはスピーカおよびプリンタなどの他の周辺出力デバイス（図示せず）を含む。

【００１１】

パーソナル・コンピュータ２０は、リモート・コンピュータ４９など１つまたは複数のリモート・コンピュータへの論理接続を使用してネットワーク化された環境内で動作する場合がある。リモート・コンピュータ４９は、他のパーソナル

・コンピュータ、サーバ、ルータ、ネットワークＰＣ、ピア・デバイス（peer device）または他の共通ネットワーク・ノードであり、典型的にはパーソナル・コンピュータに関連して上記に説明された要素の多くまたはすべてを含むことができるが、メモリ・ストレージ・デバイス５０のみが図１に示されている。図１に描かれた論理接続は、ローカルエリア・ネットワーク（ＬＡＮ）５１および広域ネットワーク（ＷＡＮ）５２を含む。このようなネットワーク化環境はオフィス、全社的コンピュータ・ネットワーク、イントラネットおよびインターネットに普通に見られる。

【００１２】

パーソナル・コンピュータ２０はＬＡＮネットワーク化環境内で使用される際には、ネットワーク・インターフェースまたはアダプタ５３を介してローカル・ネットワーク５１に接続される。パーソナル・コンピュータ２０はＷＡＮネットワーク化環境内で使用される際には、典型的にはモデム５４または他の手段を含み、インターネットなど広域ネットワーク５２上で通信を確立する。モデム５４は内部あるいは外部に置かれる場合もあるが、シリアルポート・インタフェー４６を介してシステム・バス２３に接続されている。ネットワーク化された環境では、パーソナル・コンピュータ２０またはその一部に関連して描かれたプログラム・モジュールは、リモートのメモリ・ストレージ・デバイス内に格納される場合がある。示されたネットワーク接続は例としてのものであって、コンピュータの間で通信リンクを確立する他の手段も使用できることが明らかであろう。

【００１３】

ロケーション識別

本発明の一視点によれば、（ユーザーの資格認定に基づいたユーザーの通常のアクセス権の他に）ユーザーのロケーションに基づいてリソースへのアクセスを決定する方法およびシステムが提供される。たとえば、ローカルな安全なロケーションにいると決定された有効なユーザーには彼らの完全なアクセス権を与えられるが、一方、リモートのロケーションにいるユーザーは制限付きのアクセス権を与えられる。さらに、制限の量はリモート・アクセスのタイプに基づいて変化させることもできる。

【００１４】

例として、図２はユーザーが（ローカル・マシン（複数可）を含む）企業ネットワーク６０に接続することができる、多くのロケーションを示す。ユーザーは（図１に示されたようにＬＡＮ５１およびネットワーク・インターフェース５３など）ローカルエリア・ネットワークを介してコンピュータ62_1～62_nへ接続することができる。他のユーザーはたとえばＴ１接続を介してリモートのオフィス・サーバ64_1～64_nへ接続し、さらに他のユーザーは仮想的な組織内（ＶＰＮ）６６を介してインターネットを介して接続する場合がある。さらにべつのユーザーは、任意の数のリモート・アクセス・サーバ（たとえば68_1～68_2）を介して、他のロケーション（図示せず）から多くの方法で接続できる。

【００１５】

本発明に遵守すれば、ネットワーク・リソースへアクセスするためにユーザーに許可されたアクセスのレベルは、所与のユーザーが接続した（仮想的な）ロケーションに依存する。たとえば、ＬＡＮ62_1を介してローカル・マシン６０に接続されたユーザーには完全なアクセス権を与えられるが、リモート・オフィス64_1を介したユーザーにはいくらか制限付きの権利、ＲＡＳ68_1、68_2、またはＶＰＮ６６を介したユーザーにはかなり制限付きのアクセス権を与えられる場合がある。

【００１６】

ここに使用されているように、用語「ロケーション」は、接続がそこから発生しているという距離に関連する物理的な概念ではなく、接続ロケーションのタイプに関する論理的な概念であることが容易に分かるであろう。たとえば、ユーザーは任意のタイプの電話サービスを有する、仮想的な任意の物理的なロケーションからＲＡＳ68_2を介してネットワーク６０に接続できる。同様に、ローカル・マシン６０から比較的（物理的に）遠い可能性のある「イントラネット」のロケーションから接続する場合がある。実際に、ＲＡＳ68_1、68_2ダイアルアップ・ユーザーは、Ｔ１回線を介してリモート・オフィス64_1で接続しているユーザーよりも物理的な距離においては近い可能性があるが、ダイアルアップ・ユーザーは通常は安全性が低いと考えられている。このように、ここに使用されて

いるようなロケーション、ユーザーが接続することのできる各ロケーションは、物理的なロケーションというより仮想的なロケーションと考えられる。それにもかかわらず、本発明はさらに、ユーザーの物理的なロケーションが実際に知られている場合には、物理的なロケーションに関連していくらかの動作をする場合もある（たとえば、本発明はさらに発呼者ＩＤを介して、所定のエリア・コードから呼び出すすべてのＲＡＳユーザーへアクセスを制限する場合もある）。

【００１７】

ロケーション識別を実行するために、ユーザーのロケーションを確実に決定するための機構／プロセス６７が（たとえばネットワーク・マシン６０内に）提供される。機構／プロセス６７は、１つのマシン内に種々の構成要素を備える場合もあるし、ネットワーク内の種々の構成要素の間で分散される場合もある。さらに、ここに説明されたように、ＩＰアドレスのロケーション識別に関しては２つの異なる機構がある。第１の機構はインターネット・ロケーション・サービス（ＩＬＳ）６９に基づいており、別の機構は種々のロケーションにいるクライアントに一定の範囲のＩＰアドレス（好ましくはディレクトリ・サービスによって管理されている）を割り当てること、そして信頼性のより低いロケーションから信頼性のより高いＩＰアドレスを使用することを防ぐために信頼できるルータを使用する、こと、に基づいている。どちらの方法もルーティング機構、および明確な信頼できるアクセスポイントを備えた任意のネットワーク上で機能する。

【００１８】

ユーザーが信頼できるロケーションにいないかどうかを決定する第１の（ＩＬＳ）方法は、機構６７が、そのユーザーがリモート・アクセス・サーバ（ＲＡＳ）を介して接続しているかどうかをチェックすることである。その際に、リモート・アクセス・サーバを介して接続しているのであれば、そのユーザーは、リモートで信頼性がより低い。この目的のために、図３のステップ３００によって表されたように、ＲＡＳがリモート・ユーザーのログオンを認証するとき、ＲＡＳはユーザーにインターネット・プロトコル（ＩＰ）アドレスを割り当て、このユーザーおよびＩＰアドレスをＩＬＳ（インターネット・ロケーション・サービス）６９で登録する。図３の流れ図に示すように、ＩＰアドレスがＩＬＳにリスト

されている場合（ステップ３０２）、ユーザーはこのＲＡＳクラスタを介してログオンしているので、信頼できない。このようなユーザーには、次に詳細に説明されるように、一定の削減されたアクセス・レベルを設定し（ステップ３０４）、次いでそのレベルを使用して（制限付きの）アクセス権を割り当てる（ステップ３１０）などによって、制限付きのアクセスを与えられる。

【００１９】

しかし、ユーザーのＩＰアドレスがＩＬＳ６９内でＲＡＳ　ＩＰアドレスとしてリストされていない場合、そのユーザーは必ずしもローカルでもなく信頼もできない。例として、ユーザーがヨーロッパのＲＡＳサーバを介してログオンし、次いでそこを介してＣｈａｒｌｏｔｔｅ（ノースカロライナ）ドメインへアクセスしたい場合、Ｃｈａｒｌｏｔｔｅ　ＲＡＳ　ＩＬＳはそのローカルＩＬＳにリストされたヨーロッパのＲＡＳ接続を有していない。したがって、ローカルＩＬＳ６９にリストされていないユーザーについては、ユーザーのロケーションを決定するために追加の情報が必要になる。

【００２０】

追加情報の１つの断片は割り当てられたＩＰアドレスであり、これはステップ３０６で査定される。このＩＰアドレスが、ローカル・マシンによって割り当てられたローカルな、信頼できるＩＰアドレスの範囲内にない場合、ユーザーはローカルではない。したがって、ステップ３０６における機構／プロセス６７はステップ３０４に分岐し、ここでは上記のようにレベルは信頼できないと設定される。しかしアドレスがローカルな信頼できるＩＰアドレスの範囲内にある場合、ユーザーはローカルではあってしかもＲＡＳを介して接続しておらず、したがって信頼できる。このようなユーザーには、以下に詳細に説明されるように、ユーザーに信頼できるアクセス・レベルを割り当て（ステップ３０８）、次いでそのレベルを使用してアクセス権を割り当てる（ステップ３１０）などによって、通常のアクセスが与えられる。

【００２１】

接続のための完全なルーティング・パスはサーバに使用可能であり、したがってロケーションを決定するときに、アクセスは、ユーザーのパケットがルーティ

ングされているもっとも信頼性の低いロケーション（すなわち「もっとも弱いリンク」）に基づいて割り当てられる。さらに、ＩＰアドレスが「信頼できない」ロケーションの範囲内にないとき、信頼できる範囲内にあるとは仮定されず、ロケーション識別の性質は排他的ではなく包括的であり、すなわち、信頼できるＩＰ範囲のリストは信頼できないロケーションのリストを脱落することによってレベルを割り当てるのではなく、レベルを割り当てることをテストされる。

【００２２】

他の電子セキュリティ・システムと同様に、一般に、本発明が使用される配慮のレベルはまた、全体的なセキュリティの結果についても責任を有する。たとえば、ネットワークを異なる信頼レベルで分離するときに配慮が行われるべきであり、細目は適切にルーティングされるべきであり、内部の手続きはたとえば、だれかが個人的な使用のために会社のオフィス内のデスクトップ・マシン上にＲＡＳサーバをインストールできないようにすべき、などである。

【００２３】

上記の例は簡単な、２つのレベルのローカルな識別機構６７を提供する。しかし、多数の信頼レベル制御をより細かく細分化するために、ＩＰアドレスは、ユーザーが接続しているロケーションに関する追加のロケーション情報に対応する範囲内でサーバによって割り当てられることもできる。ＲＡＳサーバはさらにロケーション識別機構７１で構成され、「許可された」電話番号からの発呼者に関しては１つの範囲で、無名のまたは登録されていない電話番号に関しては別の範囲で、ＩＰアドレスを割り当てることもできる。機構／プロセス７１は、上記の機構／プロセス６７と同じまたは同様の構成要素および追加の構成要素を含み、１つのマシン内にある場合もあり、またはネットワーク内の多くのマシンの間で分散されている場合もあることに注意されたい。しかし、より細かい細分性を提供する他に、ドメイン・サーバにおいて信頼できるＩＰアドレス範囲を維持すると、照会時にＩＬＳ６９でチェックするより時間がかからない。さらに、次に明らかになるように、全体的なセキュリティを達成するには、ロケーションマッピングへのグローバルなアドレスのデータベース、信頼できるアドレス割り当ておよび安全なルータ／ゲートウェイを含む、３つの部分の機構が一般にあることが

明らかであろう。

【００２４】

次の表は、架空の会社のために恣意的に設定された所定の方針に基づいて、ユーザーに割り当てられる可能性のある信頼レベルおよびＩＰアドレスを示したものである。ローカル・マシンへ直接（たとえばＬＡＮインターフェース・カード５３を介して）接続しているユーザーはレベル０の信頼性である。

【００２５】

【表１】

レベル	ロケーション	ＩＰアドレスの範囲
信頼レベル１	ローカルな イントラネット・ユーザ	111.22.0.0-111.22.255.255 111.24.0.0-111.24.127.255
信頼レベル２	ＲＡＳ許可ユーザー	111.24.128.255-111.24.255.255
信頼レベル３	ＲＡＳ無名ユーザー	111.25.0.0-111.25.255.255

【００２６】

例として、図４はユーザーがＲＡＳサーバ（たとえば、68_2）へ接続する際に経由するユーザー接続の、３つの異なるタイプを示す。第１のユーザーはＲＡＳ登録済み電話番号からダイアルインすることによって、リモート・コンピュータ70_1をＲＡＳサーバ68_2へ接続し、第２のユーザーは未登録またはブロックされた電話番号を介してリモート・コンピュータ70_2から接続し、第３のユーザーは任意の電話番号から接続する。最初の２人のユーザーは自分がシステムの許可されたユーザーであることを主張するユーザー認証を有するが、第３のユーザーは許可されたユーザーであると主張せず、ゲストとして接続しようとしているのみである。アクセス・レベルを決定するために、ＲＡＳサーバ68_2はまず、発呼者ＩＤ７４を介して、呼び出し側コンピュータの電話番号を決定する。電話番号が使用可能な場合（たとえば発呼者によってブロック（妨害）されていない場合）、ＲＡＳサーバ68_2は、データベース（またはテーブル）７２に問い合わせる。このデータベースは、リソースへの拡大されたアクセスを許可されて

いる登録済み電話番号のリストを保持している。　この方法で、登録済み番号から呼び出すリモート・コンピュータ７０$_1$のユーザーに対して、未登録の電話番号またはブロックされた電話番号から呼び出すリモート・コンピュータ７０$_2$のユーザーよりも、リソースへのより大きなアクセスを与えることが可能になる。さらに、７０$_1$のユーザー、７０$_2$のユーザーの双方は、ゲスト・ユーザ７０$_3$の電話番号にかかわらず、ゲスト・ユーザ７０$_3$よりも大きなアクセス権を有することが可能になる。たとえば、リモート・コンピュータ７０$_3$のユーザーは公共サーバ７６上のファイルへのアクセスのみを許可されるが、一方、未登録の番号から呼び出すユーザー・コンピュータ７０$_2$は、公共サーバ７６および従業員サーバ７８へのアクセスを有する可能性がある。最後に、登録済み番号から呼び出すユーザー・コンピュータ７０$_1$は、公共サーバ７６、従業員サーバ７８、および機密サーバ８０にアクセスを有するが、トップ・シークレットサーバ８２にはアクセスを有しない可能性がある。このような区別は、会社が任意の数のアクセス方針を設定することを可能にする。上記の例では、移動中の従業員は未登録のロケーションから呼び出して一部の従業員レベルのファイルにアクセスすることはできるが（さらに彼らのユーザー資格認定によって制限される）、しかし機密ファイルにはアクセスできないことになる。機密ファイルは、ユーザーの家または登録済み電話番号を有する他の知られたロケーションからのみアクセスでき、一方、トップ・シークレット・ファイルはどのＲＡＳ接続を介してもアクセスできない。

【００２７】

まとめると、図５～６は、既定の方針に基づいてアクセス・レベルが割り当てられる方法を示す、例としての流れ図を含む。図５のステップ５００でユーザーがローカル・マシン６０を介して接続している場合、ステップ５０２で信頼レベルは０に設定され、これは次いでステップ５１６に続き、ここではアクセス権は信頼レベルに基づいて（部分的に）割り当てられる。しかし、ローカル・マシンを介して接続していない場合、プロセス／機構７１は図６に続き、ここではリモート接続のタイプが割り当てられたＩＰアドレスを介して信頼レベルを決定する。図６のステップ５２０でユーザーがダイアルアップ接続を介して接続していな

い場合、ステップ５２０はステップ５２２へ分岐し、そのユーザーに割り当てられたＩＰアドレスは、ローカル・イントラネット・ユーザのために保存されたアドレスの範囲内である。この簡単な例では、ユーザーはローカル・マシンに直接接続するか、イントラネット接続を介するかまたはダイアルアップ接続を介して接続するかのいずれかであることに注意されたい。

【００２８】

しかし、ステップ５２０でユーザーがダイアルアップ接続を介して接続していると検出された場合、ステップ５２０はステップ５２４に分岐し、接続が行われている電話番号を決定する。この情報は発呼者ＩＤ機構７２などを介して使用可能にされる場合があることが理解されるであろう。呼び出し発生時にユーザーが発呼者ＩＤ機能をブロック（妨害）している可能性、または発呼側電話が機能を稼動できない（たとえば、発呼側電話が発呼者ＩＤを備えた領域以外のロケーションにある場合など）可能性があるため、ステップ５２６はその電話番号が使用可能かどうかをテストし、決定する。機構７２が、必要な場合には意図的にブロックされた呼び出しと、検出できないだけの呼び出しとを区別する機能がある場合、方針は２つのタイプを区別し、異なる信頼レベルを設定できることに注意されたい。しかし、ここの例では、どういう理由でも電話番号が使用可能でない場合、ステップ５２６はステップ５３２に分岐し、そこでＩＰアドレスは、ＲＡＳ未登録ユーザー範囲内で割り当てられる。

【００２９】

しかし、ステップ５２６でその番号が使用可能な場合、ステップ５２８が実行され、ここでは番号を使用してデータベース７４などを問い合わせ、その番号が既定の信頼できるロケーションとして登録済み番号であるかどうかを決定する。この時点で、ロケーション情報はオプションとしてユーザー識別と組み合わせられる場合があり、たとえば、ユーザーＸと識別されたユーザーは、彼または彼女の登録済みの家の番号から呼び出している場合には拡大されたアクセスを与えられるが、その他のユーザーはその番号から呼び出しても拡大されたアクセスを受け取らないことに注意されたい。

【００３０】

ステップ５３０によって番号が適切に登録されていると決定された場合、ステップ５３０はステップ５３４に分岐し、ここでＩＰアドレスは発呼側コンピュータに関するＲＡＳ登録済みユーザー範囲内で割り当てられる。番号が適切に登録されていると決定されなかった場合、ステップ５３０はステップ５３２に分岐し、ここでＩＰアドレスはＲＡＳ未登録ユーザー範囲内で割り当てられる。ロケーション識別プロセス／機構７１は次いで図５のステップ５０４に戻り、ここで割り当てられたアドレスはアクセス権を決定するマシンによって査定される。

【００３１】

ステップ５０４でＩＰアドレスがローカル・イントラネット・ユーザの範囲内にある場合、ステップ５０４はステップ５０６に分岐し、ここでは信頼レベルはこのユーザーについて１と設定される。ＩＰアドレスがローカル・イントラネット・ユーザの範囲内にない場合、ステップ５０８はその範囲がＲＡＳ登録済みユーザーの範囲内にあるかどうかをテストし決定する。範囲内にある場合、ステップ５１０で信頼レベルは２に設定されるが、範囲内にない場合、信頼レベルはステップ５１２で３と設定される。信頼レベルが０から３に一度設定されると、プロセスは次にステップ５１６に続き、次に詳細に説明するようにここでユーザーの資格認定の組み合わせにおけるユーザーの信頼レベルに基づいてアクセス権が割り当てられる。

【００３２】

図７は一般に、本発明によるアクセス権を決定するための論理を示す。セキュリティ・プロバイダ８８はユーザー資格認定９０およびロケーション情報（たとえば信頼レベル）９２をとり、その情報に基づいてそのユーザーのためのアクセス権９４を決定する。次に説明するように好ましい実施形態では、アクセス権はユーザーのプロセスの各々に関連付けられたアクセス・トークン内におかれ、各リソースに関連付けられたセキュリティ情報と比較されて、そのリソースへのアクセスを決定する。

【００３３】

制限付きトークンを使用したロケーションの識別

次に明らかになるように、本発明は好ましくはオペレーティング・システム・

レベルで実装され、したがって、実質的にアクセス情報に関してすべての可能性をカバーする。例として、サーバ上の所与のファイルを保護することを考えてみる。このファイルは、リモートＳＭＢファイル・アクセス、サーバ上で実行しているスクリプトを介して、サーバ上で実行しているＦＴＰサーバを介して、プロキシ（第３のマシン）を介してなど、多くの方法でアクセスできる。本発明はシステム・レベルで動作し、実質的にファイルにアクセスするすべての方法を保護することを可能にする。

【００３４】

ここに説明された本発明の好ましいセキュリティ・モデルは、既存のＷｉｎｄｏｗｓ　ＮＴセキュリティ・モデルを強化し、拡張する。しかし、本発明をＷｉｎｄｏｗｓ　ＮＴオペレーティング・システムに限定する意図はなく、逆に、本発明は、何らかの方法で入力情報に基づいてリソースへのアクセスを限定できる任意の機構で動作し、利益を与えることが目的とされている。

【００３５】

一般に、Ｗｉｎｄｏｗｓ　ＮＴオペレーティング・システムでは、ユーザーはプロセス（およびそのスレッド）を介してシステムのリソースにアクセスすることによってタスクを実行する。簡単に説明するために、プロセスおよびそのスレッドは概念上等価と見なされ、今後は簡単にプロセスと呼ぶ。また、Ｗｉｎｄｏｗｓ　ＮＴ内ではオブジェクトによって表される、ファイル、共有メモリおよび物理デバイスを含むシステムのリソースは、本明細書では通常リソースまたはオブジェクトと呼ばれる。

【００３６】

ユーザーがＷｉｎｄｏｗｓ　ＮＴオペレーティング・システムにログオンし認証されると、セキュリティ・コンテキストがそのユーザーのためにセットアップされ、この中にはアクセス・トークン１００の構築も含まれる。図８の左側に示すように、従来のユーザー・ベースのアクセス・トークン１００は、ＵｓｅｒＡｎｄＧｒｏｕｐｓフィールド１０２を含む。ＵｓｅｒＡｎｄＧｒｏｕｐｓフィールド１０２は、セキュリティ識別子、すなわち、ユーザーの証明およびそのユーザーが属するグループ（たとえば編成内のグループ）を識別する１つまたは複数

のグループＩＤ１０６に基づいたセキュリティ識別子（セキュリティＩＤまたはＳＩＤ）１０４を含むトークン１００はまた、そのユーザーに割り当てられた任意の特権を一覧する特権フィールド１０８を含む。たとえば、このような特権の１つは、管理レベルのユーザーに、特定のアプリケーション・プログラミング・インタフェース（ＡＰＩ）を介してシステム・クロックを設定する能力を与える場合がある。特権は、アクセス制御チェック、これは次に説明されるが、特権がない場合はオブジェクトへのアクセスを許可する前に実行されるアクセス制御チェックに優先することに注意されたい。

【００３７】

次に詳細に説明され、図９に一般に示されるように、オブジェクト１１２へのアクセスを所望するプロセス１１０は、所望するアクセスのタイプを指定し（たとえばファイル・オブジェクトへの読み取り／書き込みアクセスを得るなど）、および、カーネル・レベルでは関連付けられたトークン１００をオブジェクト・マネジャー１１４に提供する。オブジェクト１１２はそれに関連付けられたカーネル・レベルのセキュリティ記述子１１６を有し、オブジェクト・マネジャー１１４はセキュリティ記述子１１６およびトークン１００をセキュリティ機構１１８に提供する。セキュリティ記述子１１６の内容は、典型的にはオブジェクトの所有者（たとえば制作者）によって決定され、一般に（任意に）アクセス制御エントリーのアクセス制御リスト（ＡＣＬ）１２０を含み、各エントリーについて、そのエントリーに対応する１つまたは複数のアクセス権（許可されたアクションまたは拒否されたアクション）を含む。各エントリーはタイプ（拒否または許可）インジケータ、フラグ、セキュリティ識別子（ＳＩＤ）およびアクセス権をビット・マスクの形で含み、各ビットは許可に対応する（たとえば、１つのビットは読み取りアクセス、１つのビットは書き込みアクセス、など）。セキュリティ機構１１８はトークン１００内のセキュリティＩＤおよびプロセス１１０によって要求されたアクション（複数可）のタイプをＡＣＬ１２０内のエントリーと比較する。許可されたユーザーまたはグループに関して一致が発見され、所望のアクセスのタイプがそのユーザーまたはグループに許可可能な場合、オブジェクト１１２へのハンドルはプロセス１１０に戻されるが、その他の場合は、アクセ

スは拒否される。

【００３８】

例として、ユーザーを「会計」グループのメンバーとして識別するトークンを持つユーザーが読み取りおよび書き込みアクセスで特定のファイル・オブジェクトにアクセスしたいとする。ファイル・オブジェクトが、ＡＣＬ１２０のエントリー内で許可されたタイプの「会計」グループ識別子を有し、そのグループが読み取りおよび書き込みアクセスを使用可能にする権利を有する場合、読み取りおよび書き込みアクセスを許可するハンドルは戻されるが、その他の場合は、アクセスは拒否される。効率上の理由から、セキュリティ・チェックはプロセス１１０がまずオブジェクト１１２（作成または開く）にアクセスしようと試みたときのみ実行され、したがってそのオブジェクトに対するハンドルはそれを介して実行できるアクションを制限するように、アクセス情報のタイプを格納することに注意されたい。

【００３９】

セキュリティ識別子１１６はまた、システムＡＣＬまたはＳＡＣＬ１２１を含み、これは監査されるべきクライアント・アクションに対応するタイプ監査のエントリーを含む。各エントリー内のフラグは監査が成功したオペレーションまたは失敗したオペレーションのどちらを監視するかを示し、エントリー内のビット・マスクは監査されるべき動作のタイプを示す。エントリー内のセキュリティＩＤは、監査されているユーザーまたはグループを示す。たとえば、ファイル・オブジェクトへの書き込みアクセスを有しないグループのメンバーがそのファイルに書き込もうと試みた場合いつでも決定できるように特定のグループが監査されている状況を考えてみる。そのファイル・オブジェクトに関するＳＡＣＬ１２１は、その中にグループ・セキュリティ識別子と、適切に設定された失敗フラグおよび書き込みアクセス・ビットを有する監査エントリーを含む。その特定のグループに属するクライアントがそのファイル・オブジェクトに書き込みしようとして失敗するといつでも、そのオペレーションは記録される。

【００４０】

ＡＣＬ１２０は、（すべての権利または選択された権利に関して）グループ・

ユーザーにアクセスを許可するのではなく、アクセスを拒否するためにマークされる１つまたは複数の識別子を含む場合があることに注意されたい。たとえば、ＡＣＬ１２０内にリストされた１つのエントリーは、その他の場合には「グループ$_3$」のメンバーにオブジェクト１１２へのアクセスを許可するが、ＡＣＬ１２０内の他のエントリーは特に、「グループ$_{24}$」のすべてのアクセスを拒否する場合がある。トークン１００が「グループ$_{24}$」セキュリティＩＤを含んでいる場合、アクセスは「グループ$_3$」のセキュリティＩＤの存在にかかわらず拒否されることになる。もちろん、セキュリティ・チェックは正しく機能するために、「グループ$_3$」エントリーを介したアクセスを許可しないようにアレンジされ、その後、すべてのＤＥＮＹ（拒否）エントリーをＡＣＬ１２０の前面に置くなどによって、グループ$_{24}$エントリーの「ＤＥＮＹ　ＡＬＬ（すべて拒否）」状態をチェックする。この構成（arrangement）は、グループの残りのメンバーの各々を個別にリストしてそのアクセスを許可する必要なく、グループの、１人または複数の分離したメンバーが個別にＡＣＬ１２０内で排除できるので、向上した効率を提供することが明らかであろう。

【００４１】

アクセスのタイプを指定する代わりに、発呼者はＭＡＸＩＭＵＭ＿ＡＬＬＯＷＥＤアクセスを要求することもでき、これによって、アルゴリズムは通常のＵｓｅｒＡｎｄＧｒｏｕｐｓリスト対ＡＣＬ１２０内の各々のエントリーに基づいて、許可される最大のアクセス・タイプを決定することに注意されたい。より詳しくは、アルゴリズムは所与のユーザーのための権利を蓄積してい識別子のリストをウォーク・ダウン（すなわち、種々のビット・マスクをＯＲする）。権利が一度蓄積されると、ユーザーに蓄積された権利が与えられる。しかし、ウォーク・スルーの間にユーザー識別子またはグループ識別子および要求された権利に一致する拒否エントリーが発見されると、アクセスは拒否される。

【００４２】

制限付きトークンは（制限付きまたは制限なしのいずれかの）既存のアクセス・トークンから作成され、ユーザーの通常のトークンよりも少ないアクセスを有する（すなわち、その権利および特権のサブセットを有する）。ここに使用され

ているように、ユーザーの「通常の」トークンは、（ユーザーまたはグループを介する）ユーザーの識別に基づいてのみアクセスを許可し、他には追加の制限がないトークンである。制限付きトークンは、ユーザーの通常のトークンがこれらのＳＩＤを介してアクセスを許可ししている場合でも、特に「ＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹ」とマークされた１つまたは複数のユーザーまたはグループのセキュリティＩＤを介したリソースへのアクセスを許可されず、および／または、ユーザーの通常のトークン内にある特権を削除する場合がある。また次に説明するように、制限付きトークンが任意の制限付きセキュリティＩＤを有する場合、トークンは追加のアクセス・チェックを受け、ここで制限付きセキュリティＩＤはオブジェクトのＡＣＬ内のエントリーと比較される。

【００４３】

本発明の一態様によれば、アクセス・トークンはユーザーの識別およびユーザーが接続しているロケーションの両方に基づいて、そのユーザーのために作成される。一般に、そのロケーションの信頼性が低いと、関連付けられたプロセスがアクセスできるリソースに関して、および／または、そのトークンがこれらのリソースについて実行できるアクションに関して、そのトークンはより制限を受ける。たとえば、ＬＡＮを介して接続しているユーザーはそのユーザーのプロセスに関連付けられた通常のトークンを有する可能性があるが、一方、ＲＡＳを介して接続された同じユーザーでは、彼または彼女のプロセスはすべての特権をはぎ取られた制限付きトークンに関連付けられる可能性がある。

【００４４】

上記のように、アクセスを削減する１つの方法は、制限付きトークンの中で１つまたは複数のユーザーおよび／またはグループのセキュリティ識別子の属性を変更して、アクセスを許可するのではなくアクセスを許可できないようにすることである。ＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹとマークされたセキュリティＩＤは、アクセスを許可する目的のためには効果的に無視されるが、そのセキュリティＩＤに関して「ＤＥＮＹ（拒否）」エントリーを有するＡＣＬは、依然としてアクセスが拒否される。例として、制限付きトークン１２４（図９）内のグループ$_2$のセキュリティＩＤがＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹとマークされ

ている場合、ユーザーのプロセスが、グループ$_2$を許可されたものとしてリストしているＡＣＬ１２０を有するオブジェクト１１２へアクセスしようと試みたとき、このエントリーは効果的に無視され、プロセスは他の何らかのセキュリティＩＤによってアクセスを得なければならないことになる。しかし、ＡＣＬ８０が要求されたタイプのアクションに関してグループ$_2$をＤＥＮＹとしてリストしているエントリーを含んでいる場合、一度テストされると、他のセキュリティＩＤにかかわらずアクセスは許可されない。

【００４５】

これはサーバに、ユーザーまたはグループがユーザーのロケーションに基づいてオブジェクトへアクセスすることを制限する能力を与えることが理解されるであろう。上記のように、ＩＰアドレス範囲はユーザーのロケーションに基づいて、たとえば、ローカル・マシンへ接続している場合は信頼レベル０、イントラネットまたは他の信頼できるロケーションから接続している場合は信頼レベル１、許可された電話番号からＲＡＳを介している場合はレベル２、その他の場合はレベル３と指定できる。このアドレスの範囲は次いで検査され、所定のグループをＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹとマークする。

【００４６】

例として、それぞれ、（それらのＡＣＬに基づいて）トップ・シークレット・ファイル、機密ファイル、従業員ファイルへアクセスを許可する、「トップ・シークレット」ＳＩＤ、「機密」ＳＩＤ、および「従業員」ＳＩＤを含む通常のアクセス・トークンを有するユーザーＸとして識別されたユーザーを考えてみる。ユーザーＸが信頼レベル０であった場合、ユーザーＸの通常のトークンが使用され、そこにはロケーションに基づいた制限はない。しかし、信頼レベル１では、トップ・シークレットＳＩＤは、ユーザーＸのアクセス・トークンの中でＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹとマークされる。同様に、信頼レベル２では、トップ・シークレットＳＩＤおよび機密ＳＩＤの両方がＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹとマークされ、一方、レベル３では、トップ・シークレットＳＩＤ、機密ＳＩＤおよび従業員ＳＩＤがＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹとマークされる。セキュリティＩＤは一部のオブジェクトのＡＣＬ内では「ＤＥＮＹ」と

してマークされ、その識別子を削除すると、これらのオブジェクトへのアクセスを拒否するのではなく許可することになるため、セキュリティＩＤをユーザーのトークンから削除するだけでは、オブジェクトへのアクセスを安全に削減できないことに注意されたい。さらに、このＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹセキュリティ・チェックをオフにする機構は提供されていない。

【００４７】

制限付きトークン内でアクセスを削減する別の方法は、親トークンに関連する１つまたは複数の特権を削除することである。たとえば、管理特権を伴う通常のトークンを有するユーザーは、ユーザーがローカル・マシン６０に直接接続されていない限り、ユーザーのプロセスがまったく特権を有しないか、何らかの方法で削減された特権を有する制限付きトークンで実行するように、本発明のロケーションに基づいたシステムを介して制限することができる。残る特権はまた、たとえば、ローカル（レベル０）の場合はすべての特権、レベル１の場合は一部の特権、レベル２または３の場合はまったく特権なしなど、信頼のレベルに基づいている場合があることが理解されるであろう。

【００４８】

ユーザーのロケーションに基づいてトークンのアクセスを削減するさらに別の方法は、そこに制限付きセキュリティＩＤを追加することである。制限付きセキュリティＩＤは、プロセス、リソース動作などを表す番号であり、ＧＵＩＤに接頭部または、暗号ハッシュなどを介して生成された番号を追加するなどによってユニークになっており、これらのセキュリティＩＤを他のセキュリティＩＤから区別するための情報を含むことができる。以下に説明するように、トークンが制限付きのセキュリティＩＤを含む場合、そのトークンは追加のアクセス・チェックを受け、ここで制限付きセキュリティＩＤはオブジェクトのＡＣＬ内のエントリーに対して比較される。したがって、たとえば制限付きＳＩＤは「ＲＡＳ」を指定し、これによって、オブジェクトのＡＣＬが「ＲＡＳ」エントリーを有しないかぎり、ユーザーはそのオブジェクトへのアクセスを拒否されることになる。

【００４９】

図９に示されたように、制限付きセキュリティＩＤは制限付きトークン１２４

の特別なフィールド１２２に置かれ、本発明によって、プロセスがアクションを要求するロケーションを識別することができる。以下に詳細に説明されるように、少なくとも１つのユーザー（またはグループ）セキュリティＩＤおよび少なくとも１つの制限付きセキュリティＩＤがそのオブジェクトへのアクセスを許可されるように要求することによって、オブジェクトはそのロケーション（同時にユーザーまたはグループ）に基づいて選択的にアクセスを許可できる。さらに、ロケーションの各々は異なるアクセス権を許可される場合もある。

【００５０】

この設計は、ユーザーが所与のロケーションから実行を許可されていることを制御するため、ユーザーのコンテキストに重要な融通性および細分性を与える。例として、ローカル・マシンに接続しているユーザーはレベル０の信頼性、イントラネットおよび信頼できるロケーションから接続しているユーザーはレベル１の信頼性、（ＲＡＳを通じて）許可された電話番号およびインターネットから接続しているユーザーはレベル２の信頼性、および制限付きのロケーションまたは許可されていない電話番号から接続しているユーザーはレベル３の信頼性である、上記の例を考えてみる。すると、ユーザーのロケーションに基づいて（たとえば、ユーザーのＩＰアドレスから確かめられたように）、レベル０からレベル３の信頼性を、次のように実行される何らかの既定の方針に基づいて定義することができる。

【００５１】

【表２】

57

レベル	セキュリティ・コンテキスト内での制限
０	ユーザーのセキュリティ・コンテキストに追加の制限はない
１	ユーザーは、たとえば、バックアップ／復元など非常に微妙な動作から除去された特権を有するなど、制限付きコンテキストの基でオペレーションを実行する。
２	ユーザーは、すべてのＳＩＤが依然として実行可能だが、特権を有しない制限付きコンテキストの元でオペレーションを実行する。
３	ユーザーは、制限付きコンテキストの元で操作し、制限付きコンテキストは、たとえば、全員および認証されたユーザーなど一定の人をのぞいて、ＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹビットを使用してすべてのＳＩＤが使用不可能になっている。すべての特権はレベル２と同じように除去されている。

【００５２】

既存のトークンから制限付きトークンを作成するために、ＮｔＦｉｌｔｅｒＴｏｋｅｎと名付けられたアプリケーション・プログラミング・インターフェース（ＡＰＩ）が提供され、その内容は次のとおりである。

【００５３】

【表３】

```
NTSTATUS
NtFilterToken (
        IN HANDLE ExistingTokenHandle,
        IN ULONG Flags,
        IN PTOKEN_GROUP SideToDisable OPTIONAL,
        IN PTOKEN_PRIVILEGS PrivilegeToDelete OPTIONAL,
        IN PTOKEN_GROUP RestrictingSids OPTIONAL,
        OUT PHANDLE NewTokenHandle
        );
```

【００５４】

ＮｔＦｉｌｔｅｒＴｏｋｅｎ　ＡＰＩは、ＣｒｅａｔｅＲｅｓｔｒｉｃｔｅｄＴｏｋｅｎと名付けられたＷｉｎ３２　ＡＰＩの下でラップされ、Ｃｒｅａｔｅ

ＲｅｓｔｒｉｃｔｅｄＴｏｋｅｎの内容は次のとおりである。

【００５５】

【表４】

```
WINADVAPI
BOOL
APIENTRY
CreateRestrictedToken(
      IN HANDLE ExistingTokenHandle,
      IN DWORD Flags,
      IN DWORD DisableSidCount,
      IN PSID_AND_ATTRIBUTES SidsToDisable OPTIONAL,
      IN DWORD DeletePrivilegeCount,
      IN PLUID_AND_ATTRIBUTES PrivilegesToDelete OPTIONAL,
      IN DWORD RestrictedSidCount,
      IN PSID_AND_ATTRIBUTES SidsToRestrict OPTIONAL,
      OUT PHANDLE NewTokenHandle
      );
```

【００５６】

図８および図１０～１１に表示されたように、これらのＡＰＩ１２６は共同して機能し、制限付きでも制限なしでも既存のトークン１００をとり、変更された（制限付き）トークン１２４をそこから作成する。ログオンしたユーザーのインスタンスに関する識別情報を含む制限付きトークンの構造は、ＰａｒｅｎｔＴｏｋｅｎＩｄ，ＲｅｓｔｒｉｃｔｅｄＳｉｄＣｏｕｎｔ、およびＲｅｓｔｒｉｃｔｅｄＳｉｄｓの３つの新しいフィールドを含む（次の表で太字で示されている）。

【００５７】

【表５】

61

```
Typedef struct _TOKEN {
 TOKEN_SOURCE TokenSource;                    // Ro: 16-Bytes
 LUID TokenId;                                // Ro: 8-Bytes
 LUID AuthenticationId;                       // Ro: 8-Bytes
 LUID ParentTokenId;                          // Ro: 8-Bytes
 LARGE_INTEGER ExpirationTime;                // Ro: 8-Bytes
 LUID ModifiedId;                             // Wr: 8-Bytes

 ULONG UserAndGroupCount;                     // Ro: 4-Bytes
 ULONG RestrictedSidCount;                    // Ro: 4-Bytes
 ULONG PrivilegeCount;                        // Ro: 4-Bytes
 ULONG VariableLength;                        // Ro: 4-Bytes
 ULONG DynamicCharged;                        // Ro: 4-Bytes

 ULONG DynamicAvailable;                      // Wr: 4-Bytes (Mod)
 ULONG DefaultOwnerIndex;                     // Wr: 4-Bytes (Mod)
 PSID_AND_ATTRIBUTES UserAndGroups;           // Wr: 4-Bytes (Mod)
 PSID_AND_ATTRIBUTES RestrictedSids;          // Ro: 4-Bytes
 PSID PrimaryGroup;                           // Wr: 4-Bytes (Mod)
 PLUID_AND_ATTRIBUTES Privileges;             // Wr: 4-Bytes (Mod)
 PULONG DynamicPart;                          // Wr: 4-Bytes (Mod)
 PACL DefaultDacl;                            // Wr: 4-Bytes (Mod)

 TOKEN_TYPE TokenType;                        // Ro: 1-Byte
```

【００５８】

【表６】

```
 SECURITY_IMPERSONATION_LEVEL
                      ImpersonationLevel; // Ro: 1-Byte

 UCHAR TokenFlags;                        // Ro: 4-Bytes
 BOOLEAN TokenInUse;                      // Wr: 1-Byte

 PSECURITY_TOKEN_PROXY_DATA ProxyData;    // Ro: 4-Bytes
 PSECURITY_TOKEN_AUDIT_DATA AuditData;    // Ro: 4-Bytes
 ULONG VariablePart;                      // Wr: 4-Bytes (Mod)
} TOKEN, * PTOKEN;
```

【００５９】

通常の（制限なしの）トークンがＣｒｅａｔｅＴｏｋｅｎ　ＡＰＩを介して作成されるとき、ＲｅｓｔｒｉｃｔｅｄＳｉｄｓフィールドもＰａｒｅｎｔＴｏｋｅｎＩｄフィールドも空であることに注意されたい。

【００６０】

制限付きトークン１２４を作成するために、このプロセスは適切なフラグ設定および／または入力フィールドの情報を伴うＣｒｅａｔｅＲｅｓｔｒｉｃｔｅｄ

Ｔｏｋｅｎ　ＡＰＩを呼び出し、これはＮｔＦｉｌｔｅｒＴｏｋｅｎ　ＡＰＩを順番に起動する。図１０のステップ１０００の初めに示すように、ＮｔＦｉｌｔｅｒＴｏｋｅｎ　ＡＰＩは、ＤＩＳＡＢＬＥ＿ＭＡＸ＿ＳＩＤＳと名付けられたフラグが設定されているかどうかをチェックする。このフラグは、新しい、制限付きトークン１２４の中にあるグループに関してすべてのセキュリティＩＤがＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹとマークされていなければならないことを示す。このフラグは、各々のグループを個別に識別する必要なく、トークン内のグループ（多くのグループである可能性がある）に制限を行う便利な方法を提供する。フラグが設定されている場合、ステップ１０００はステップ１００２に分岐し、ステップ１００２では新しいトークン１２４内のグループ・セキュリティＩＤの各々について、ＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹを示すビットを設定する。

【００６１】

ＤＩＳＡＢＬＥ＿ＭＡＸ＿ＳＩＤＳフラグが設定されていない場合、ステップ１０００はステップ１００４に分岐し、ＮｔＦｉｌｔｅｒＴｏｋｅｎ　ＡＰＩのＳｉｄｓＴｏＤｉｓａｂｌｅフィールド内にセキュリティＩＤが個別にリストされているかどうかをテストする。図１０のステップ１００４で示されたように、オプションのＳｉｄｓＴｏＤｉｓａｂｌｅ入力フィールドが存在するとき、ステップ１００６では、そこにリストされ、また、親トークン１００のＵｓｅｒＡｎｄＧｒｏｕｐｓフィールド１０２内にも存在する任意のセキュリティＩＤは、新しい制限付きトークン１２４のＵｓｅｒＡｎｄＧｒｏｕｐｓフィールド１２８内でＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹとして個別にマークされる。上記のようにこのようなセキュリティＩＤは、アクセスを拒否するためにのみ使用でき、アクセスを許可するためには使用できず、さらに、あとから削除または使用可能にはできない。したがって、図８に示された例では、グループ$_2$のセキュリティＩＤは、ＮｔＦｉｌｔｅｒＴｏｋｅｎ　ＡＰＩ１２６のＳｉｄｓＴｏＤｉｓａｂｌｅ入力フィールド内にグループ$_2$セキュリティＩＤを指定することにより、制限付きトークン１２４内でＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹとしてマークされる。

【００６２】

フィルタ・プロセスはついで図１０のステップ１０１０に続き、ここではＤＩＳＡＢＬＥ＿ＭＡＸ＿ＰＲＩＶＩＬＥＤＧＥＳと名付けられたフラグがテストされる。このフラグは同様に、新しい、制限付きトークン１２４内のすべての特権を削除すべきであることを示す、便利なショートカットとして設定できる。このように設定された場合、ステップ１０１０はステップ１０１２に分岐し、ステップ１０１２では新しいトークン１２４からすべての特権が削除される。

【００６３】

フラグが設定されていない場合、ステップ１０１０はステップ１０１４に分岐し、ここではオプションのＰｒｉｖｉｌｅｇｅｓＴｏＤｅｌｅｔｅフィールドが確認される。ＮｔＦｉｌｔｅｒＴｏｋｅｎ　ＡＰＩ１２６が呼ばれたときに存在する場合は、ステップ１０１６で、この入力フィールドにリストされ、また既存のトークン１００の特権フィールド１０８にも存在する任意の特権は、新しいトークン１２４の特権フィールド１３０から個別に削除される。図８に示された例では、「特権$_2$」から「特権$_m$」として示された特権は、ＮｔＦｉｌｔｅｒＴｏｋｅｎ　ＡＰＩ１２６のＰｒｉｖｉｌｅｇｅｓＴｏＤｅｌｅｔｅ入力フィールド内にこれらの特権を指定することによって、新しいトークン１２４の特権フィールド１３０から削除されている。上記のように本発明の１つの態様によれば、これは、トークン内で使用可能な特権を削減する機能を提供する。このプロセスは図１１のステップ１０２０に続く。

【００６４】

制限付きトークン１２４を作成するときに、ステップ１０２０でＲｅｓｔｒｉｃｔｉｎｇＳｉｄｓ入力フィールド内にＳＩＤが存在していた場合、親トークンが通常のトークンか、または親トークン自体が制限付きＳＩＤを有する制限付きトークンであるかどうかに関して決定が行われる。ＡＰＩ、ＩｓＴｏｋｅｎＲｅｓｔｒｉｃｔｅｄがステップ１０２２で呼び出され、親トークンのＲｅｓｔｒｉｃｔｉｎｇＳｉｄｓフィールドを（ＮｔＱｕｅｒｙＩｎｆｏｒｍａｔｉｏｎＴｏｋｅｎ　ＡＰＩを介して）照会してこれがＮＵＬＬでないかどうかを確認することによってこの問題を解決し、ここでＮＵＬＬでなかった場合、親トークンは制

限付きトークンであり、ＡＰＩはＴＲＵＥ（真）を戻す。テストが満足できなかった場合、親トークンは通常のトークンでありＡＰＩはＦＡＬＳＥ（偽）を戻す。続くステップ１０２６または１０２８のために、トークン自体は制限付きであるが制限付きＳＩＤを有しない親トークン（すなわち、特権が削除されているかおよび／またはＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹ　ＳＩＤＳである場合）は、制限付きでないとして処理される可能性があることに注意されたい。

【００６５】

ステップ１０２４では、親トークンが制限付きである場合、ステップ１０２４はステップ１０２６に分岐し、ステップ１０２６では、親トークンの制限付きセキュリティＩＤフィールドと、ＡＰＩの制限付きセキュリティＩＤ入力リストの両方にある任意のセキュリティＩＤは、新しいトークン１２４の制限付きセキュリティＩＤフィールド１３２に置かれる。制限付きセキュリティＩＤが両方のリストになければならないため、制限付き実行コンテキストが、制限付きセキュリティＩＤフィールド１３２にさらなるセキュリティＩＤを追加することを阻止し、この場合、アクセスを減らすのではなく効果的にアクセスを増やすことになる。同様に、ステップ１０２６で共通なセキュリティＩＤがなかった場合、少なくとも１つの制限付きＳＩＤを新しいトークン内の元のトークンから取り去るなどによって、作成された任意のトークンはそのアクセスを増やすことなく制限されなければならない。その他の場合は、新しいトークン内の空の制限付きＳＩＤフィールドはそのトークンが制限されていないことを示し、この場合、アクセスを減らすのではなく効果的にアクセスを増やすことになる。

【００６６】

あるいは、ステップ１０２４で親トークンが通常のトークンであると判断された場合、ステップ１０２８で新しいトークン１２４のＲｅｓｔｒｉｃｔｉｎｇＳｉｄｓフィールド１３２は入力フィールド内にリストされたものに設定される。これはセキュリティＩＤを追加するが、次に詳細に説明されるように制限付きＳＩＤを有するトークンが第２のアクセス・テストを受けるため、アクセスは実際には減らされることに注意されたい。

【００６７】

最後に、ステップ１０３０も実行され、ここで新しいトークン１２４内のＰａｒｅｎｔＴｏｋｅｎＩｄ９３は既存の（親）トークンのＴｏｋｅｎＩｄに設定される。これはオペレーティング・システムに、通常は親トークン以外には許可されていないロケーションで、そのトークンの制限付きのバージョンを使用するプロセスをのちに許可するオプションを提供する。

【００６８】

特に図１２～１４を参照して本発明の動作の説明に戻ると、図１２に表示されたように、制限付きプロセス１３４が作成され、読み取り／書き込みアクセスでファイル・オブジェクト１１０を開こうと試みている。オブジェクト１１２のセキュリティ記述子内では、ＡＣＬ１２０はそこにリストされた多くのセキュリティＩＤおよび、各ＩＤに関して許可されたタイプのアクセスを有し、ここで「ＲＯ」は読み取りのみのアクセスが許可されていることを示し、「ＷＲ」は読み取り／書き込みアクセスを示し、「ＳＹＮＣ」は同期化アクセスが許可されていることを示す。他の場合は「ＸＪｏｎｅｓ」が許可されたグループ内のメンバーシップを介してアクセスを許可されている場合でも、「ＸＪｏｎｅｓ」は特にオブジェクト１１２へのアクセスを拒否されていることに注意されたい。さらに、関連付けられたこのトークン１２４を有するプロセス９４は、このエントリーは「ＤＥＮＹ」（すなわち、ＵＳＥ＿ＦＯＲ＿ＤＥＮＹ＿ＯＮＬＹ）とマークされているため、トークン１２４内の「バスケットボール」セキュリティＩＤを介して任意のオブジェクトへのアクセスを許可されないことになる。

【００６９】

図１２に表されているように、制限付きセキュリティ・コンテキストは第１にＷｉｎｄｏｗｓ　ＮＴカーネル内で実装される。オブジェクト１１２へのアクセスを試みるために、プロセス１３４はオブジェクト・マネジャー１１４に、アクセスが所望されているオブジェクトを識別する情報および、所望されるアクセスのタイプを提供する（図１４、ステップ１４００）。オブジェクト・マネジャー１１４はこれに応答して、ステップ１４０２に表されたように、セキュリティ機構１１８と共同して機能し、トークン１２４内にリストされた（プロセス１３４と関連付けられている）ユーザーおよびグループ・セキュリティＩＤをＡＣＬ１

２０内のエントリーと比較し、所望のアクセスが許可されるべきか拒否されるべきかを決定する。

【００７０】

ステップ１４０４で一般に示されているように、アクセスがリストされたユーザーまたはグループに関して許可されていない場合、セキュリティ・チェックはステップ１４１４でアクセスを拒否する。しかし、ステップ１４０４でアクセス・チェックのユーザー部分およびグループ部分の結果が許可可能なアクセスを示した場合には、セキュリティ・プロセスはステップ１４０６に分岐し、制限付きトークン１２４が任意の制限付きセキュリティＩＤを有しているかどうかを決定する。有していない場合、追加の制限はなく、ここでアクセス・チェックは完了し、ステップ１４１２において、ユーザー・アクセスおよびグループ・アクセスのみに基づいてアクセスは許可される（そのオブジェクトへのハンドルが戻される）。このようにして、通常のトークンは本質的に以前と同じようにチェックされる。しかし、ステップ１４０６によって決定されたように、トークンが制限付きセキュリティＩＤを含んでいる場合、ついでステップ１４０８によって、制限付きセキュリティＩＤをＡＣＬ１２０内のエントリーと比較することによって、第２のアクセス・チェックが実行される。ステップ１４１０でこの第２のアクセス・テストがアクセスを許可した場合、そのオブジェクトへのアクセスはステップ１４１２で許可される。そうでない場合、アクセスはステップ１４１４で拒否される。

【００７１】

図１３で論理的に示すように、トークン１２４の中に制限付きセキュリティＩＤが存在するときはいつでも、２部分からなるテストがこのように実行される。トークン１２４内のセキュリティＩＤおよび所望のアクセス・ビット１３６をオブジェクト１１２のセキュリティ記述子に対して考慮することによって、通常のアクセス・テスト（ビットごとのＡＮＤ）および制限付きセキュリティＩＤのアクセス・テストの両方は、プロセスがそのオブジェクトへのアクセスを許可されるようにアクセスを許可しなければならない。本発明に必要ではないが上記のように、通常のアクセス・テストが最初に行われ、アクセスが拒否された場合には

、さらなるテストは必要ではない。トークン内にＡＣＬの識別子に一致するセキュリティＩＤがないため、またはＡＣＬエントリーが特に、その中にあるセキュリティ識別子に基づいてトークンへのアクセスを拒否したためのどちらの理由でも、アクセスは拒否されることに注意されたい。別法としては、トークンを制限付きＳＩＤの多数の組を有するように構成し、たとえば、組Ａ　ＯＲ（組Ｂ　ＡＮＤ組Ｃ）がアクセスを許可するなど、これらのＳＩＤの査定をカバーするさらに複雑なブール式を伴う場合もある。

【００７２】

このように図１２に示された例では、トークン１２４（フィールド１３２）内の制限付きＳＩＤのみが「インターネット・エクスプローラ」を識別する一方、オブジェクトのＡＣＬ１２０内には対応する制限付きＳＩＤがないため、図１２に示された例では、オブジェクト１１２へのアクセスはプロセス９４へは許可されない。ユーザーは通常のトークンで実行するプロセスを介してオブジェクトへアクセスする権利を有していたが、プロセス９４はＡＣＬ内に「インターネット・エクスプローラ」ＳＩＤ（非ＤＥＮＹ）を有するオブジェクトのみにアクセスできるようにするように、制限された。

【００７３】

アクセスのタイプを指定する代わりに、発呼者が指定されたＭＡＸＩＭＵＭ＿ＡＬＬＯＷＥＤアクセスを有する場合、これによって上記のように、アルゴリズムは最大のアクセスを決定するＡＣＬ１２０をウォーク・スルーする。制限付きトークンで、１つでも任意のタイプのユーザー・アクセスまたはグループ・アクセスが許可された場合、ユーザーおよびグループの実行に続いて許可可能なアクセス権のタイプ（複数可）は、第２の実行に関して所望のアクセスとして指定され、第２の実行はＲｅｓｔｒｉｃｔｅｄＳｉｄｓリストをチェックする。このようにして、制限付きトークンは通常のアクセスより少ないかまたは等しいアクセスを許可されることが確認される。

【００７４】

最後に、アクセス・トークンはロケーションに基づいた基準以外の基準に従ってさらに制限できることに注意されたい。実際には、制限付きトークンは、リソ

ースへアクセスしようとしているプロセス（たとえばマイクロソフト・エクセル）の識別を含む他の基準に基づいて制限付きセキュリティ・コンテキストを設定することを可能にする。さらに、種々の基準を組み合わせてアクセス権を決定することができる。従って、たとえばユーザーがマイクロソフト・ワードではなくマイクロソフト・エクセルを介してファイルを開いている場合、ネットワーク・ファイルへのＲＡＳのアクセスが許可される場合がある。セキュリティ識別のためには事実上、ロケーションに基づいた基準と他の基準の、無限の組み合わせが可能である。

【００７５】

認証

本発明の一態様によれば、クライアントがサーバに接続しているとき、サーバはクライアントを認証し、クライアントの識別およびロケーション情報に基づいてそのユーザーのためのトークンを構築する。たとえば図１５および１６に示されているように、よく知られたタイプの認証（すなわちＮＴＬＭ）では、クライアント・ユーザ２００はユーザーＩＤを含む認証２０２をサーバ２０４に提供し、サーバ２０４は次いでドメイン・サーバ２０６と通信してユーザーの暗号化され、格納されたパスワードに基づいてそのユーザーに関して質問を作成する。図１５に表されたように、サーバ２０４はその質問をクライアント２０２に戻し、クライアントが正しく応答する場合は、そのユーザーは認証される。

【００７６】

しかし本発明によれば、ユーザーに関して通常のトークンを構築するのみではなく、上に詳細に説明されたようにユーザー情報はセキュリティ・サブ・システム／プロバイダ２１０によってロケーション情報２０８と組み合わせられ、制限付きトークン２１２を作成する。制限付きトークン２１２は、任意のクライアント・プロセス２１６のためにサーバ２０４で実行されている各プロセスと関係付けられている。

【００７７】

図１７および１８に示されたように、Ｋｅｒｂｅｒｏｓプロトコルを含む他の認証プロトコルもまた本発明と共に使用できる。Ｋｅｒｂｅｒｏｓプロトコルに

よれば、サーバ２２０への接続の認証はチケット２２２を介して達成される。チケット２２２は、最初はキー配布センタ（ＫＤＣ）２２６として知られているネットワーク上のチケット発行機能からクライアント２２４によって受け取られる。チケット２２２はしばらくの間再使用可能であり、これによってセッションが終わった場合でも、チケット２２２が依然として有効な間は、クライアント１３０は認証プロセスを繰り返す必要はない。

【００７８】

本発明によれば、上に詳細に説明されたように（クライアント２２４によってそこに置かれた制限を含む）チケット２２２内の情報は、サーバのセキュリティ・サブ・システム／プロバイダ２２８によってユーザーのロケーション情報２３０と組み合わせられ、制限付きトークン２３２を作成する。制限付きトークン２３２は任意のクライアント・プロセス２３６のためにサーバ２２０において実行されている各プロセス２３４と関連付けられる。

【００７９】

同様に図１９および２０は、ＳＳＬとして知られている別の認証プロトコルを示す。ＳＳＬでは、クライアント・ユーザ２４０はまず公開キーに基づいた認証を使用して証明２４６から証明ＩＤ２４２を得る。サーバ２４８が認証機関２４６を信頼していると仮定して、クライアント・ユーザ２４０は証明ＩＤ２４２を使用してサーバ２４８へのアクセスを得る。図１９に表されたように、サーバ２４８とクライアント２４０の間に往復の通信が起こり、これを介してサーバはこの証明ＩＤ２４２が正しいユーザーに属していることを証明できる。

【００８０】

証明ＩＤ２４２は、ユーザーが、サーバ２４８が接続しているネットワークでアカウントを有していると識別するユーザー情報を含む。その情報は、そのユーザーのために維持されたユーザー情報（たとえばセキュリティＩＤ、グループＩＤ特権など）を有するデータベース２５０へアクセスするために使用される。次いで、上に詳細に説明されたように本発明によればデータベース２５０からのユーザー情報は、サーバのセキュリティ・サブ・システム／プロバイダ２５４によってロケーション情報２５２と組み合わせられて、制限付きトークン２５６を作

成する。制限付きトークン２５６は任意のクライアント・プロセス２６０のためにサーバ２４８において実行されている各プロセス２５８と関連付けられる。

【００８１】

これらの認証プロトコルおよび別の認証プロトコルを介して得られたユーザー情報はロケーション情報と組み合わせられて、ユーザーのリソースへのアクセスを制限することが理解されたであろう。さらに、認証のタイプ自体をユーザーのロケーションに依存させることもできる。たとえば、セキュリティを増加するためにリモート接続がＫｅｒｂｅｒｏｓまたはＳＳＬ認証を必要とし、一方、ローカル接続を介して接続しているユーザーを認証するには質疑応答認証で十分である場合もある。サーバがロケーション情報へのアクセスを有するため、サーバは特定のロケーションについて必要とされる認証のタイプを決定できる。同様に、認証のタイプはアクセス権を識別するために使用することもできる。たとえば、ＳＳＬユーザーのアクセス権は１つの方法で制限し、Ｋｅｒｂｅｒｏｓユーザーは別の方法で、ＮＴＬＭユーザーはさらに別の方法で制限することもできる。上記の方法では、制限付きトークンはユーザーの仮想的なロケーションおよび／または認証タイプに基づいて制限付きセキュリティ・コンテキストを実装する便利な機構を提供するが、他の実施形態機構も可能である。

【００８２】

本発明は種々の変形および代替の構成を可能にするが、そのうち所定の図示された実施形態が図に示され、上記に詳細に説明された。しかし、本発明を開示された具体的な形に制限する意図はなく、逆に、本発明の精神と範囲に含まれるすべての変形例、代替の構成、等価物をカバーすることが目的であることを理解されたい。

【図面の簡単な説明】

【図１】

本発明が組み入れられるコンピュータ・システムを表す構成図である。

【図２】

ユーザーがネットワークに接続する可能性のある仮想的なロケーションを一般に表す構成図である。

【図３】

本発明の一態様による、ユーザーのロケーションを決定し、そのロケーションに基づいてユーザーのアクセス・レベルを決定するために取られる一般的なステップを表す流れ図である。

【図４】

本発明の一態様による、ロケーション情報に基づいてユーザー・アクセスを確立するための種々の構成要素を一般に表す構成図である。

【図５】

本発明の一態様による、ロケーション情報に基づいてユーザーの信頼のレベルを決定するためにとられる一般的なステップを表す流れ図である。

【図６】

本発明の一態様による、ロケーション情報に基づいてユーザーの信頼のレベルを決定するためにとられる一般的なステップを表す流れ図である。

【図７】

本発明の一態様による、ユーザーのアクセス権を決定する機構を一般に表す構成図である。

【図８】

本発明の一態様による、既存のトークンから制限付きトークンを作成することを一般に表す構成図である。

【図９】

プロセスがリソースにアクセスできるかどうかを決定するための種々の構成要素を一般に表す構成図である。

【図１０】

本発明の一態様による、既存のトークンから制限付きトークンを作成するためにとられる一般的なステップを表す流れ図である。

【図１１】

本発明の一態様による、既存のトークンから制限付きトークンを作成するためにとられる一般的なステップを表す流れ図である。

【図１２】

本発明の一態様による、リソースへのアクセスを試み、関連付けられた制限付きトークンを有するプロセスを一般に表す構成図である。

【図１３】

本発明の一態様による、関連付けられた制限付きトークンを有するプロセスのオブジェクトへのアクセスを決定するための論理を一般に表す構成図である。

【図１４】

本発明の一態様による、リソースへのプロセスアクセスを許可するかどうかを決定するときにとられる一般的なステップを表す流れ図である。

【図１５】

質疑応答認証プロトコル内でクライアントとサーバの間の通信を表す図である。

【図１６】

本発明の一態様による、認証証明およびロケーション識別に基づいて制限付きトークンを作成することを表す構成図である。

【図１７】

Ｋｅｒｂｅｒｏｓ認証プロトコルに従って、サーバにおいてクライアントを認証するための通信を表す図である。

【図１８】

本発明の一態様による、認証チケットおよびロケーション識別に基づいて制限付きトークンを作成することを表す構成図である。

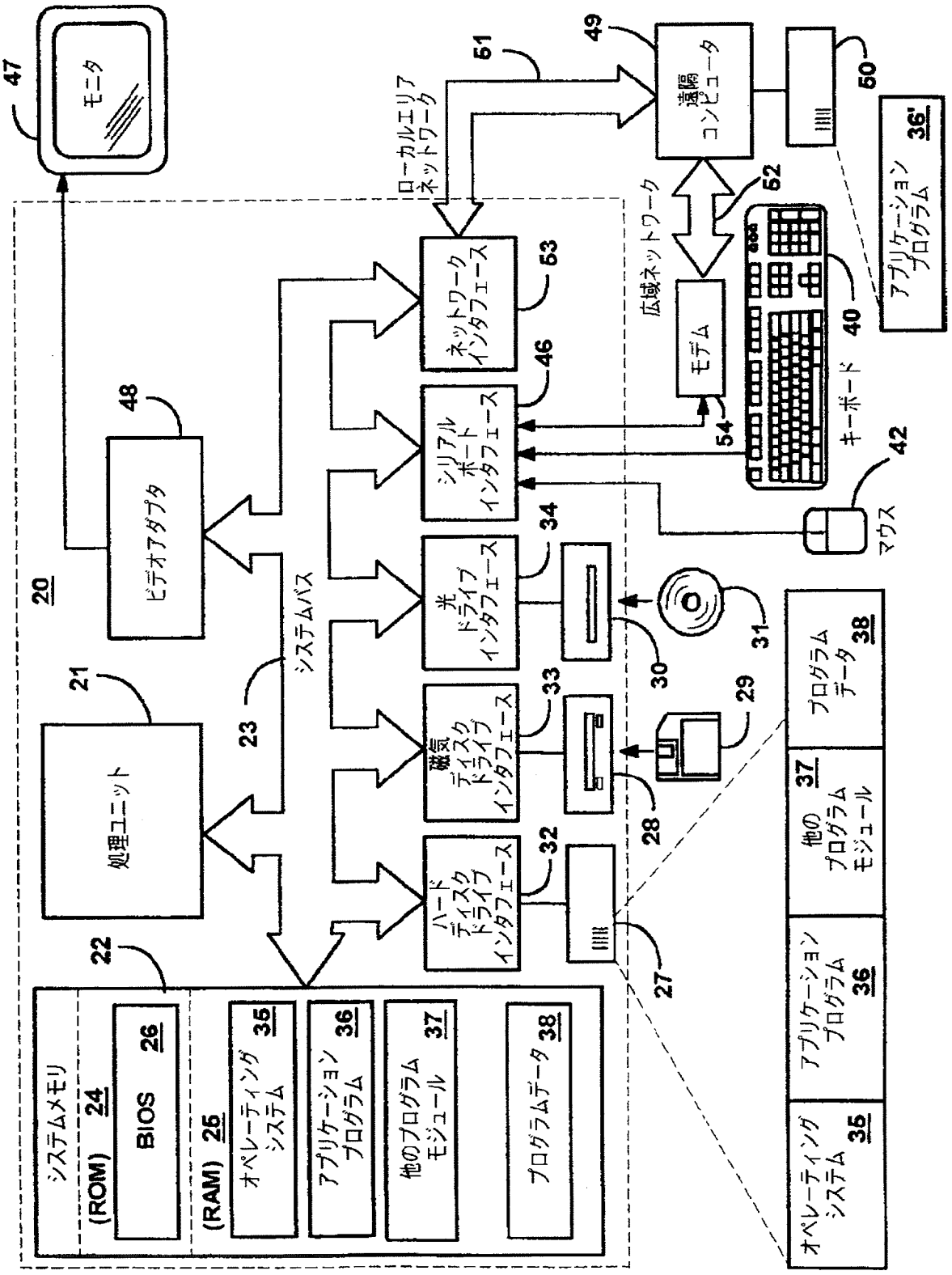
【図１９】

ＳＳＬプロトコルに従って、サーバにおいてクライアントを認証するための通信を表す図である。

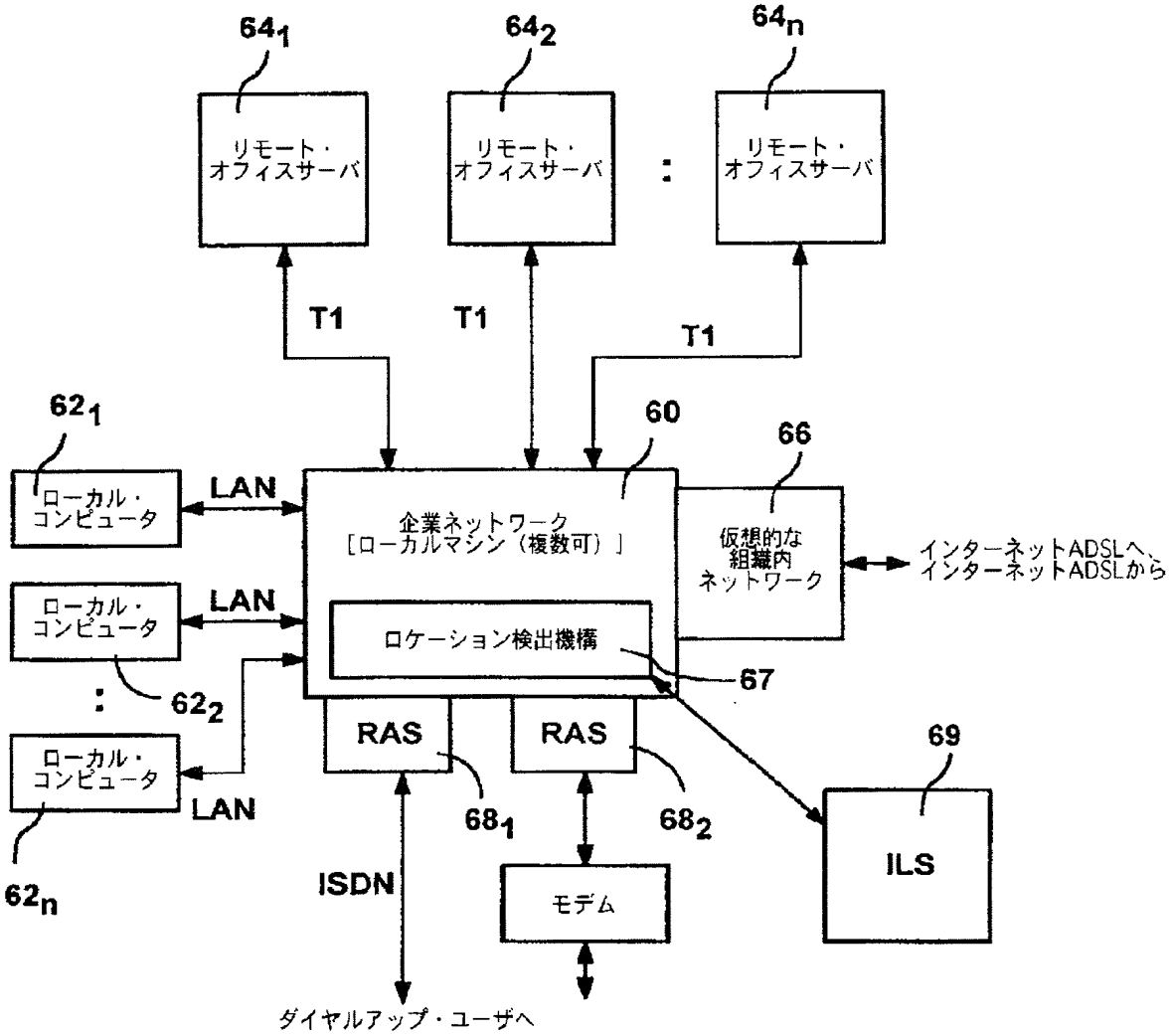
【図２０】

本発明の一態様による、認証証明およびロケーション識別に基づいて制限付きトークンを作成することを表す構成図である。

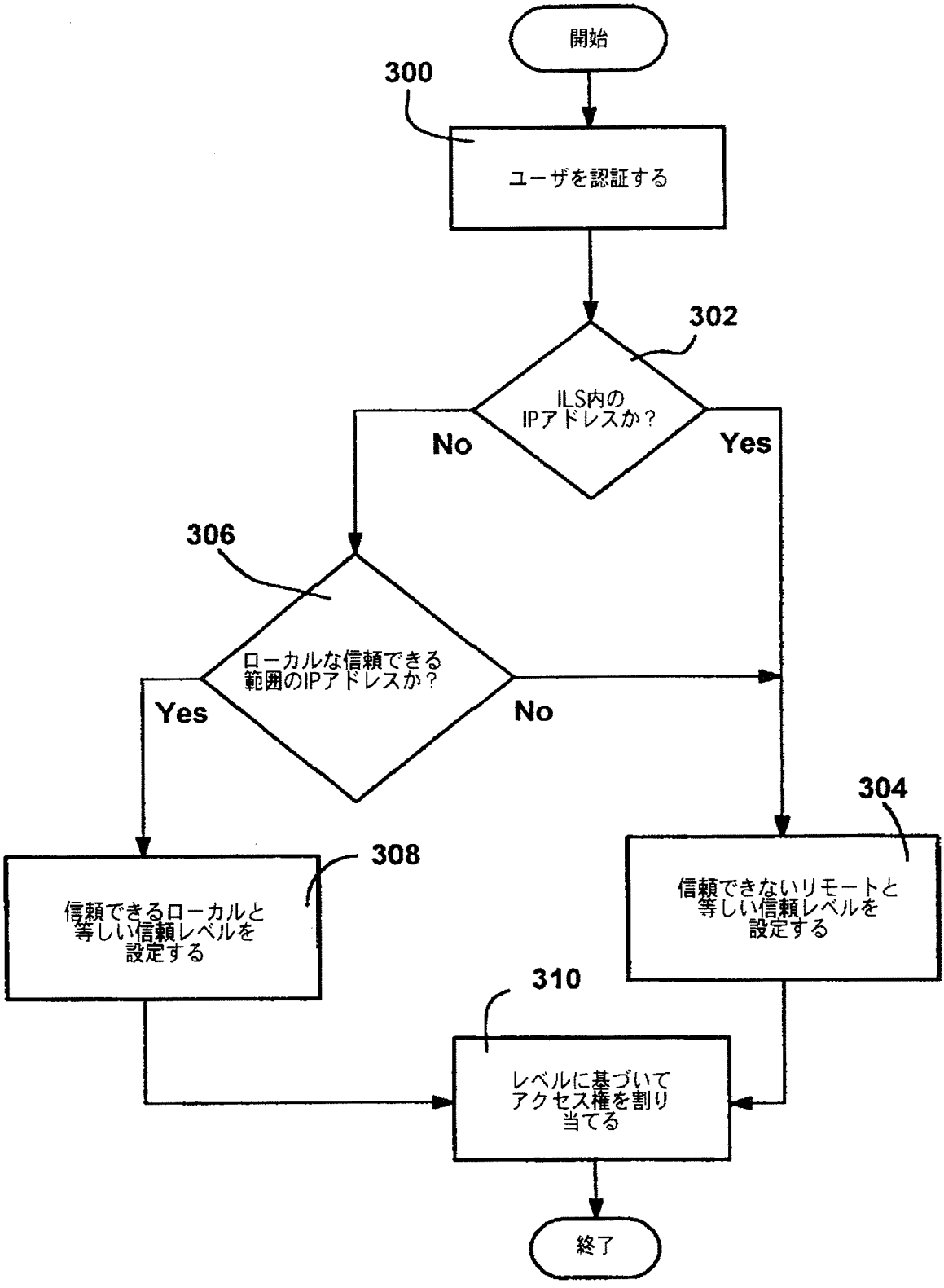
【図１】


モニタ
47
ローカルエリア
ネットワーク
51
遠隔
コンピュータ
49
50
アプリケーション
プログラム
36'
広域ネットワーク
62
モデム
54
キーボード
40
42
マウス
ネットワーク
インタフェース
53
46
シリアル
ポート
インタフェース
34
光
ドライブ
インタフェース
33
磁気
ディスク
ドライブ
インタフェース
32
ハード
ディスク
ドライブ
インタフェース
31
30
29
28
27
ビデオアダプタ
48
20
処理ユニット
21
23
システムバス
22
システムメモリ
(ROM) 24
BIOS 26
(RAM) 25
オペレーティング
システム 35
アプリケーション
プログラム 36
他のプログラム
モジュール 37
プログラムデータ 38
プログラム
データ 38
他の
プログラム
モジュール 37
アプリケーション
プログラム
36
オペレーティング
システム
35

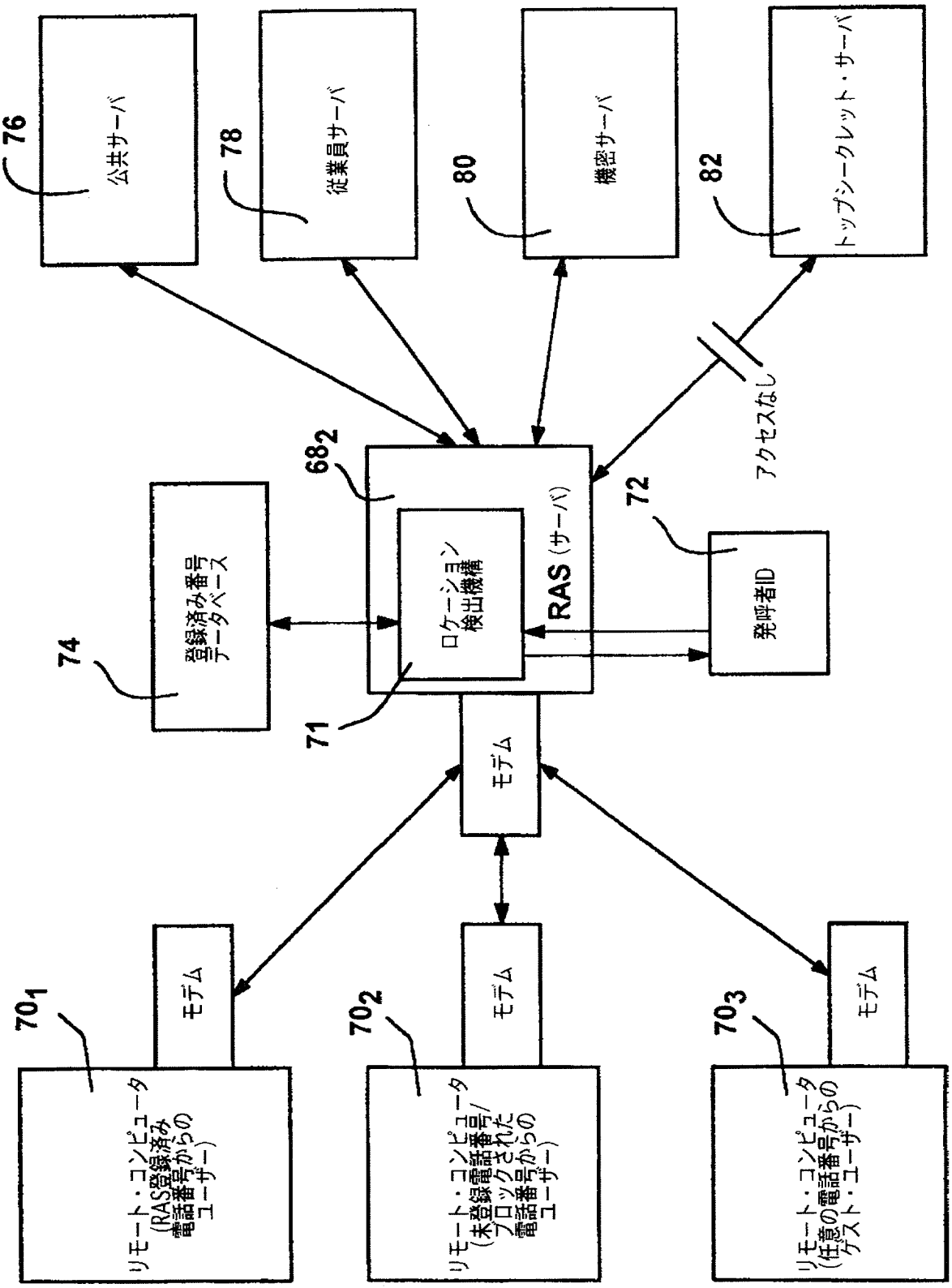
【図２】


64₁
64₂
64n
リモート・
オフィスサーバ
リモート・
オフィスサーバ
リモート・
オフィスサーバ
T1
T1
T1
62₁
60
66
ローカル・
コンピュータ
LAN
企業ネットワーク
［ローカルマシン（複数可）］
仮想的な
組織内
ネットワーク
インターネットADSLへ、
インターネットADSLから
ローカル・
コンピュータ
LAN
ロケーション検出機構
62₂
67
RAS
RAS
69
ローカル・
コンピュータ
LAN
68₁
68₂
62n
ISDN
モデム
ILS
ダイヤルアップ・ユーザへ

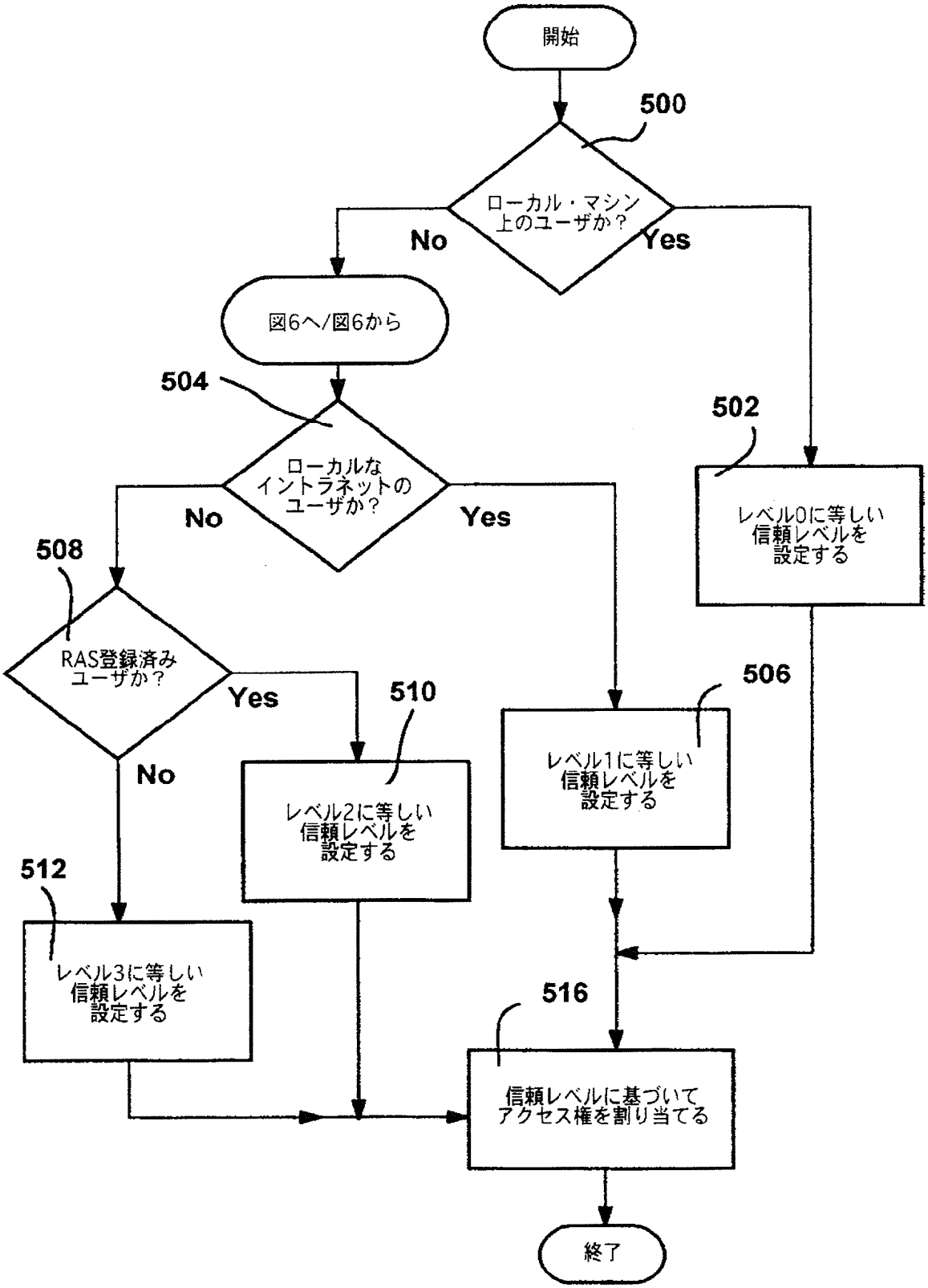
【図３】


開始
300
ユーザを認証する
302
ILS内の
IPアドレスか？
No
Yes
306
ローカルな信頼できる
範囲のIPアドレスか？
Yes
No
304
308
信頼できるローカルと
等しい信頼レベルを
設定する
信頼できないリモートと
等しい信頼レベルを
設定する
310
レベルに基づいて
アクセス権を割り
当てる
終了

【図４】


76
公共サーバ
78
従業員サーバ
80
機密サーバ
82
トップシークレット・サーバ
アクセスなし
68₂
RAS（サーバ）
ロケーション検出機構
72
発呼者ID
74
登録済み番号データベース
71
モデム
モデム
モデム
モデム
70₁
リモート・コンピュータ（RAS登録済み電話番号からのユーザー）
70₂
リモート・コンピュータ（未登録電話番号/ブロックされた電話番号からのユーザー）
70₃
リモート・コンピュータ（任意の電話番号からのゲスト・ユーザー）

【図５】


開始
500
ローカル・マシン上のユーザか？
No
Yes
図6へ/図6から
504
ローカルなイントラネットのユーザか？
No
Yes
502
レベル0に等しい信頼レベルを設定する
508
RAS登録済みユーザか？
Yes
No
510
レベル2に等しい信頼レベルを設定する
506
レベル1に等しい信頼レベルを設定する
512
レベル3に等しい信頼レベルを設定する
516
信頼レベルに基づいてアクセス権を割り当てる
終了

【図６】

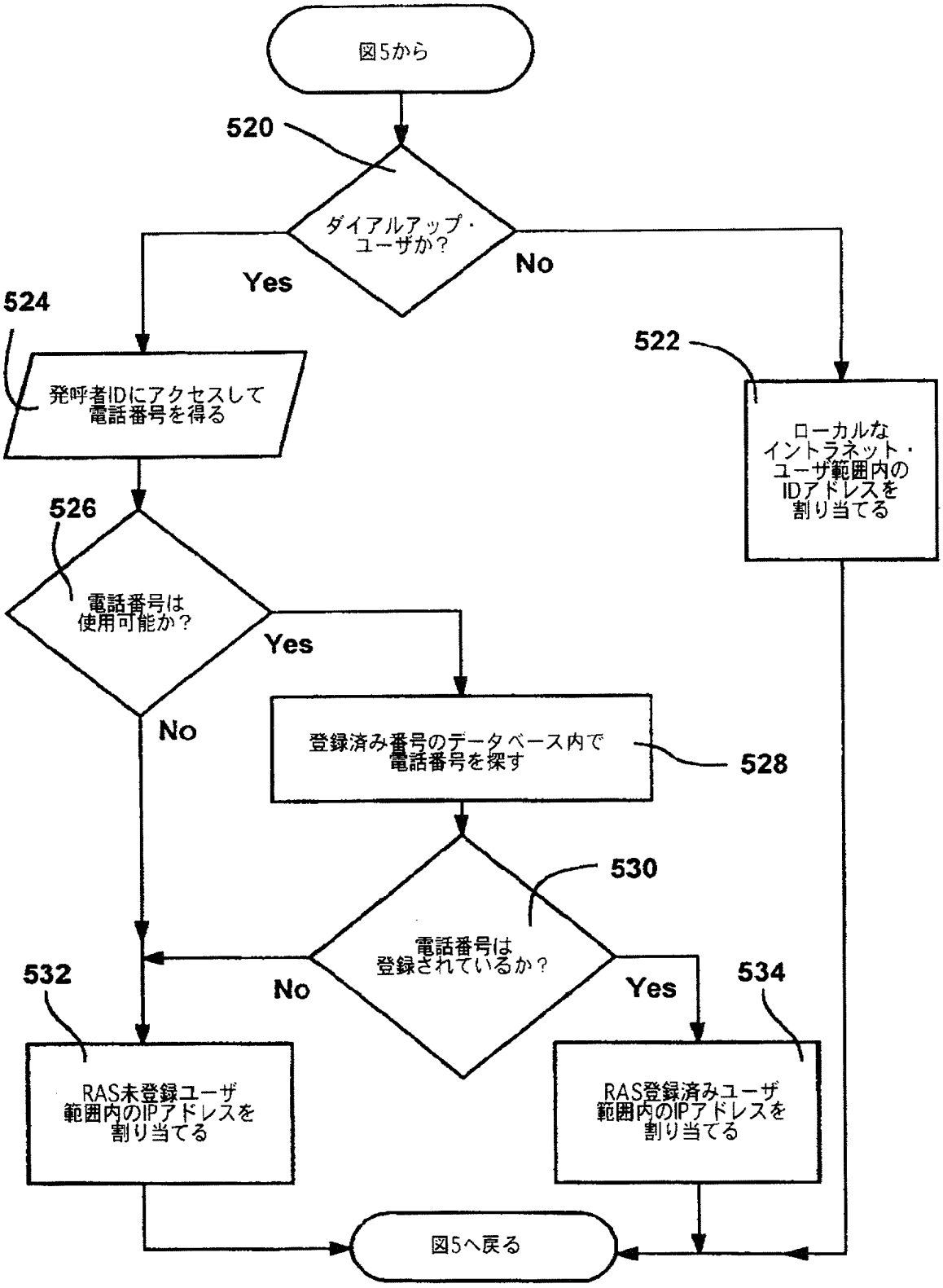
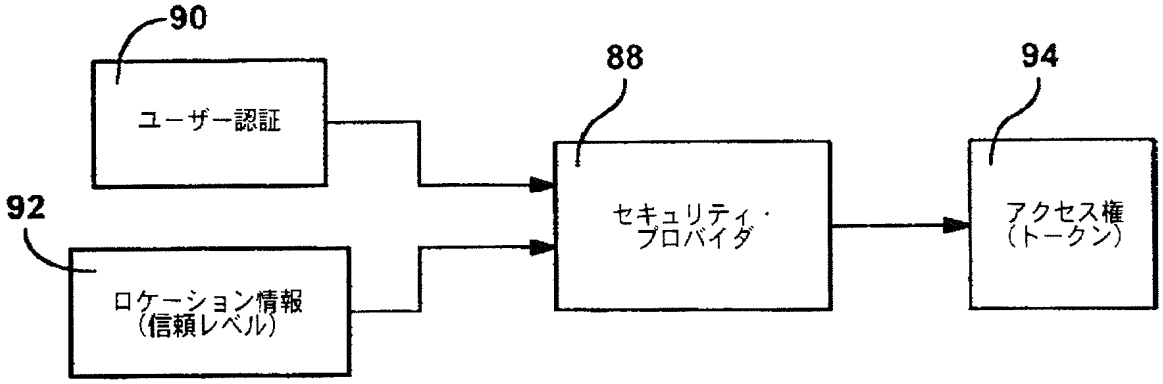
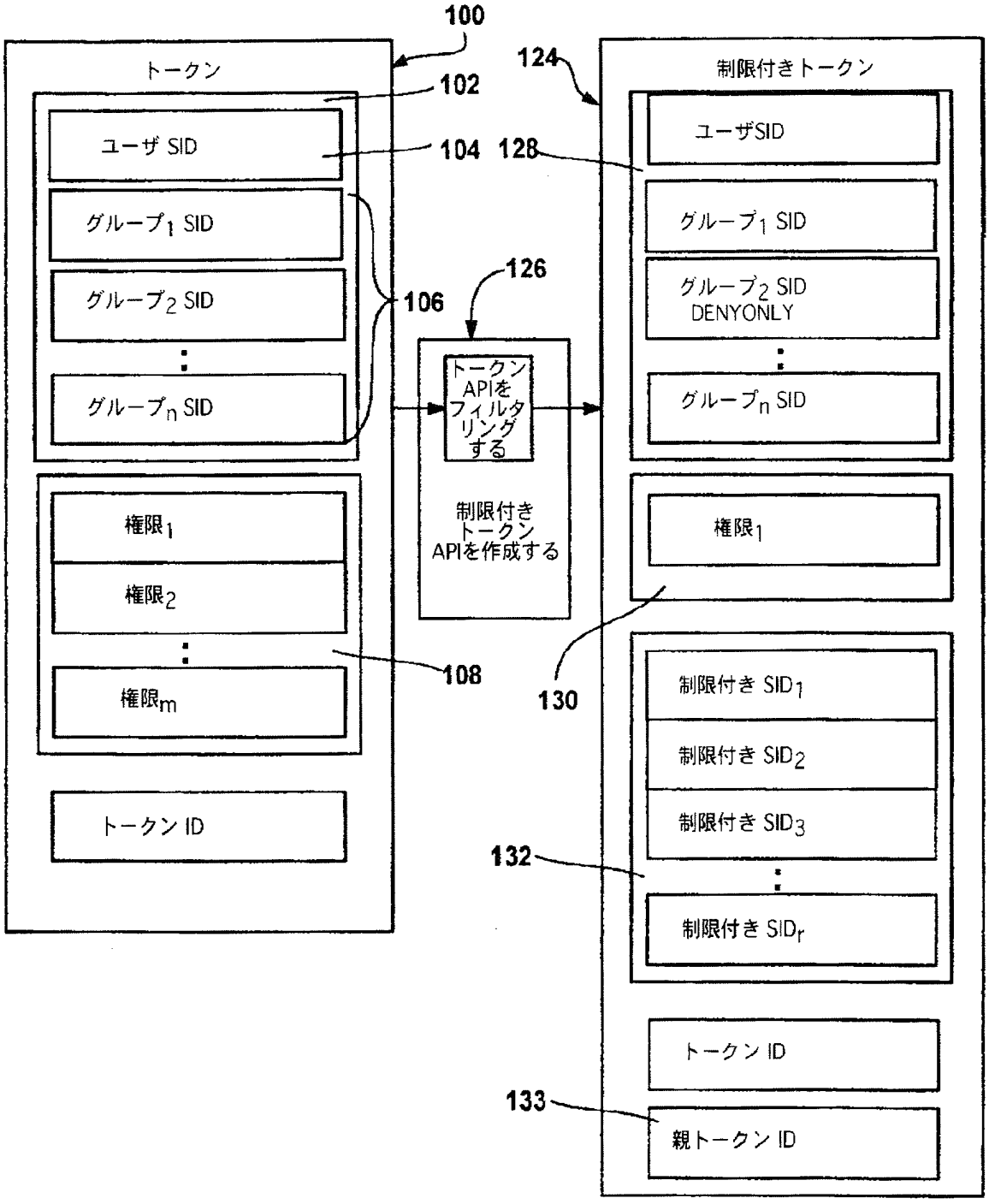


図5から
520
ダイアルアップ・
ユーザか？
Yes
No
524
発呼者IDにアクセスして
電話番号を得る
522
ローカルな
イントラネット・
ユーザ範囲内の
IDアドレスを
割り当てる
526
電話番号は
使用可能か？
Yes
No
登録済み番号のデータベース内で
電話番号を探す
528
530
電話番号は
登録されているか？
No
Yes
532
534
RAS未登録ユーザ
範囲内のIPアドレスを
割り当てる
RAS登録済みユーザ
範囲内のIPアドレスを
割り当てる
図5へ戻る

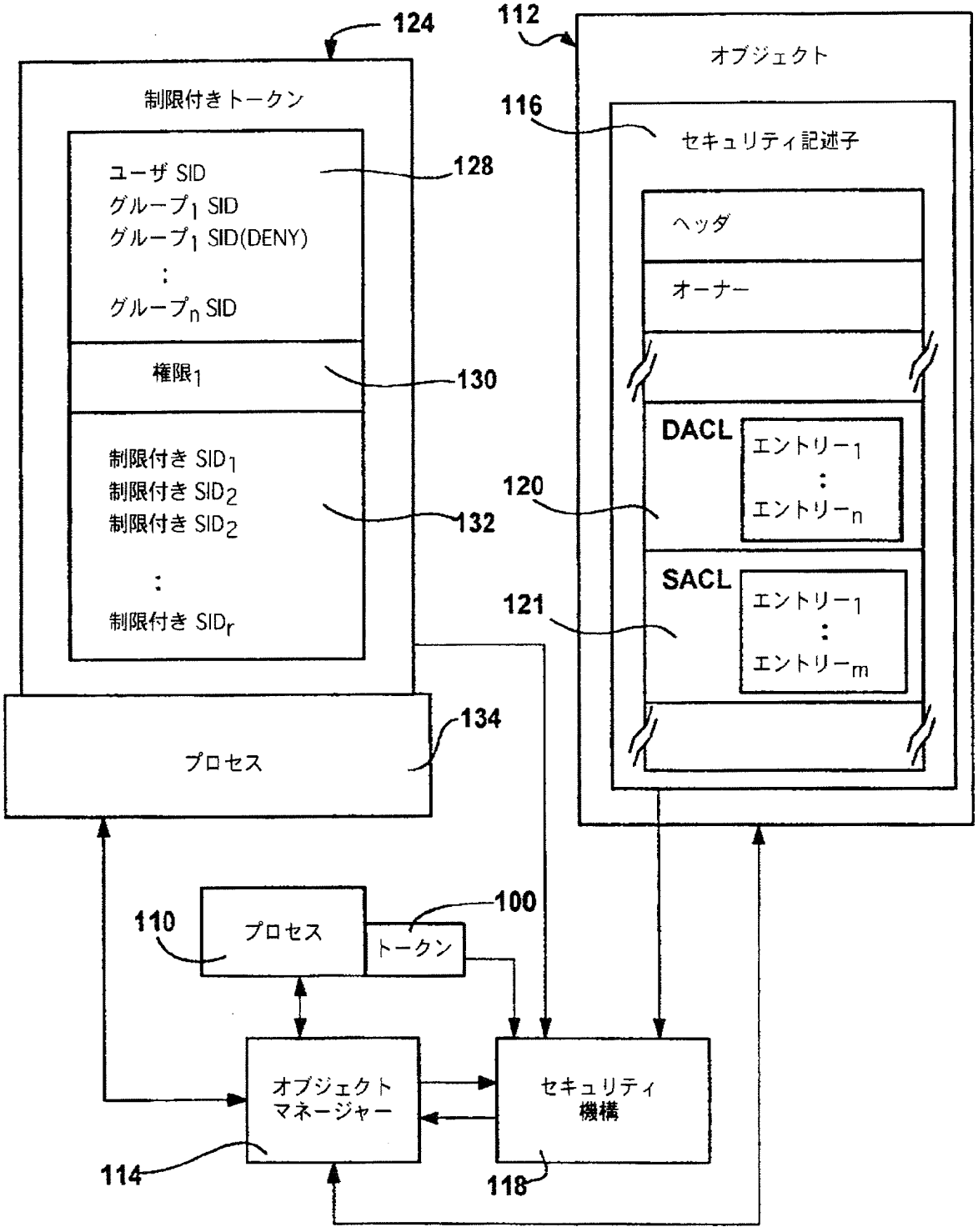
【図７】



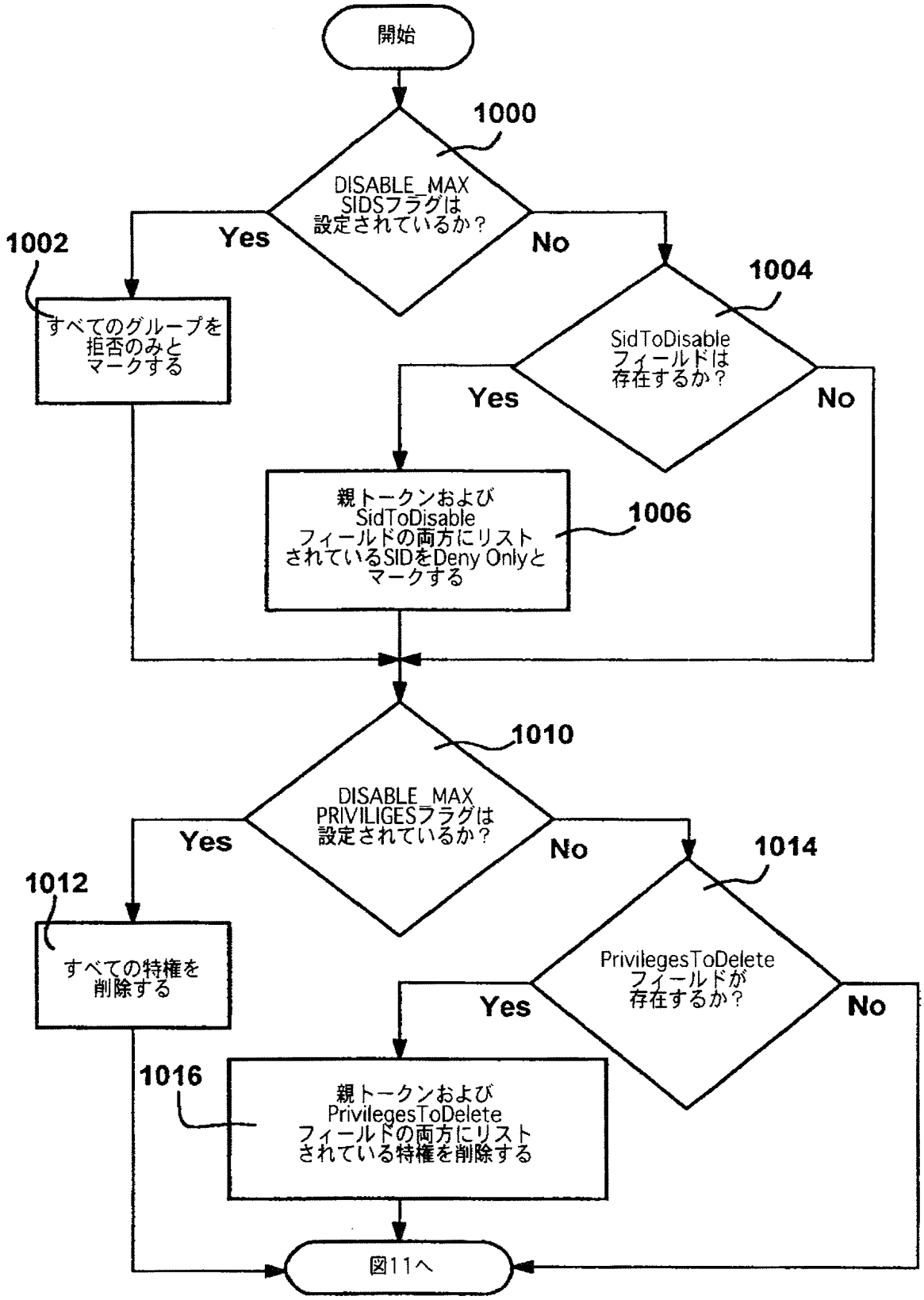
【図８】


100
トークン
102
ユーザ SID
104
グループ1 SID
グループ2 SID
106
グループn SID
126
トークンAPIをフィルタリングする
制限付きトークンAPIを作成する
権限1
権限2
108
権限m
トークン ID
124
制限付きトークン
ユーザSID
128
グループ1 SID
グループ2 SID DENYONLY
グループn SID
権限1
130
制限付き SID1
制限付き SID2
制限付き SID3
132
制限付き SIDr
トークン ID
133
親トークン ID

【図９】


124
112
制限付きトークン
オブジェクト
116
セキュリティ記述子
ユーザ SID
グループ1 SID
グループ1 SID(DENY)
:
グループn SID
128
ヘッダ
オーナー
権限1
130
DACL
エントリー1
:
エントリーn
120
制限付き SID1
制限付き SID2
制限付き SID2
:
制限付き SIDr
132
SACL
121
エントリー1
:
エントリーm
134
プロセス
110
プロセス
100
トークン
オブジェクト
マネージャー
セキュリティ
機構
114
118

【図１０】


開始
1000
DISABLE_MAX
SIDSフラグは
設定されているか？
Yes
No
1002
すべてのグループを
拒否のみと
マークする
1004
SidToDisable
フィールドは
存在するか？
Yes
No
親トークンおよび
SidToDisable
フィールドの両方にリスト
されているSIDをDeny Onlyと
マークする
1006
1010
DISABLE_MAX
PRIVILIGESフラグは
設定されているか？
Yes
No
1012
すべての特権を
削除する
1014
PrivilegesToDelete
フィールドが
存在するか？
Yes
No
1016
親トークンおよび
PrivilegesToDelete
フィールドの両方にリスト
されている特権を削除する
図11へ

【図１１】

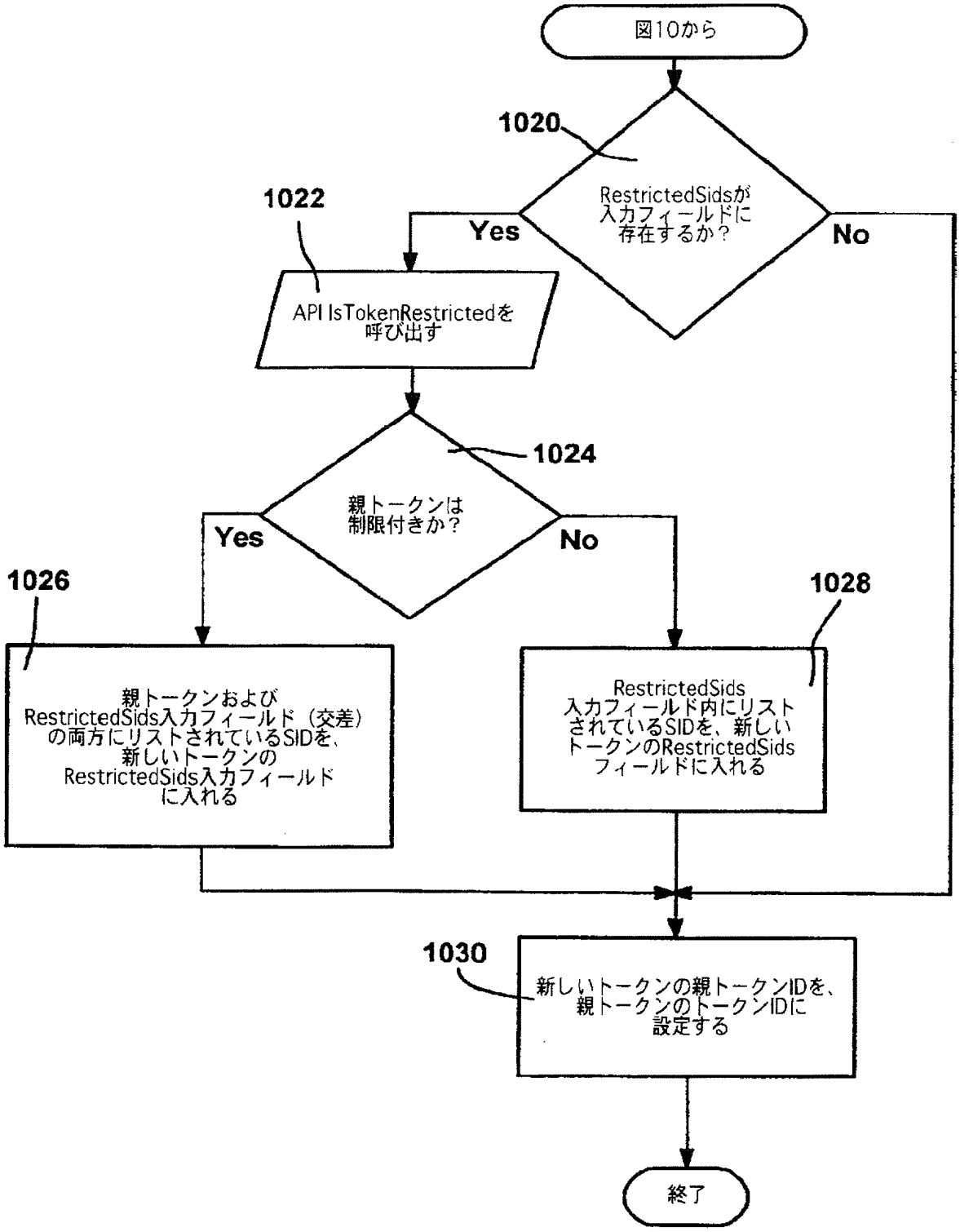
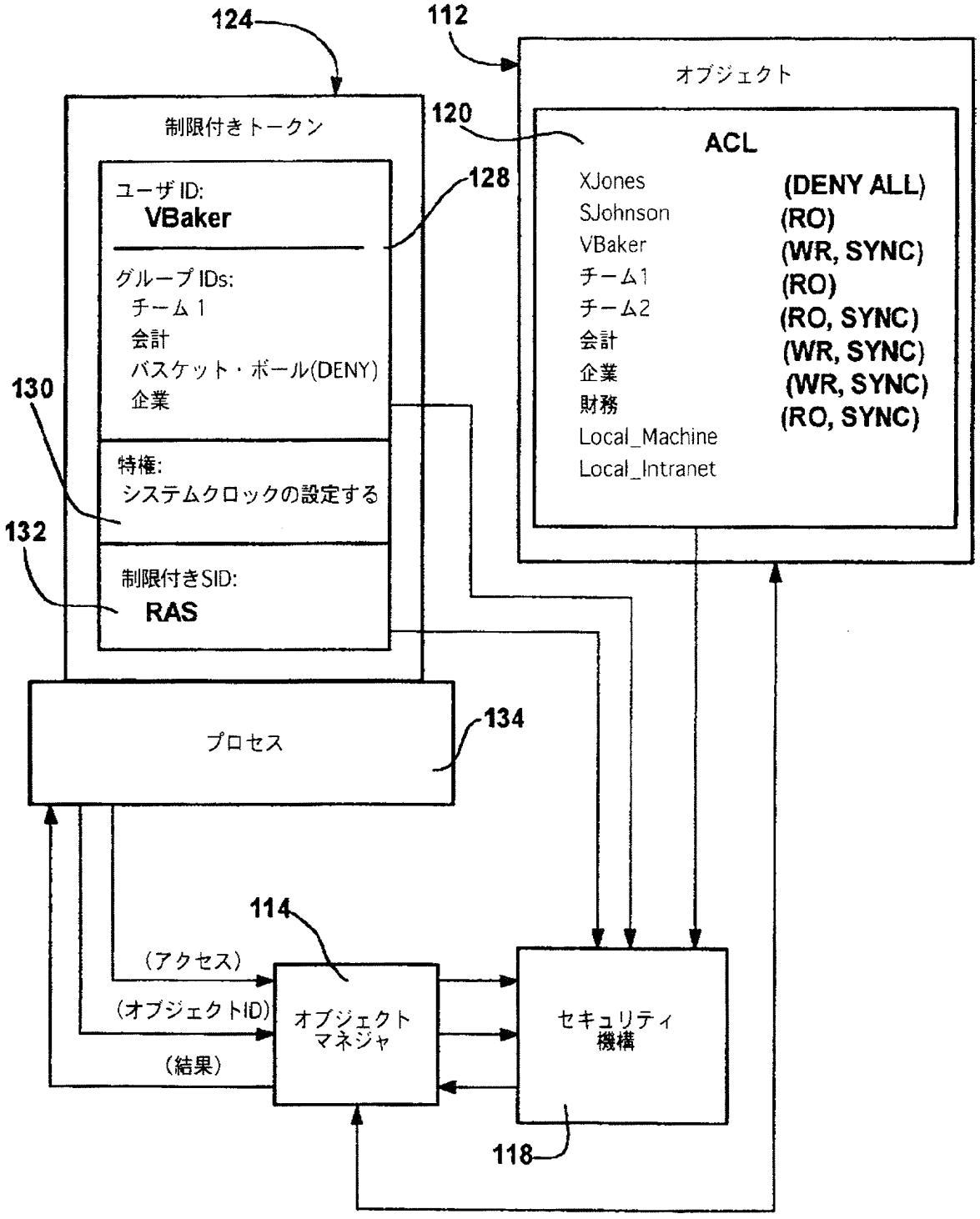
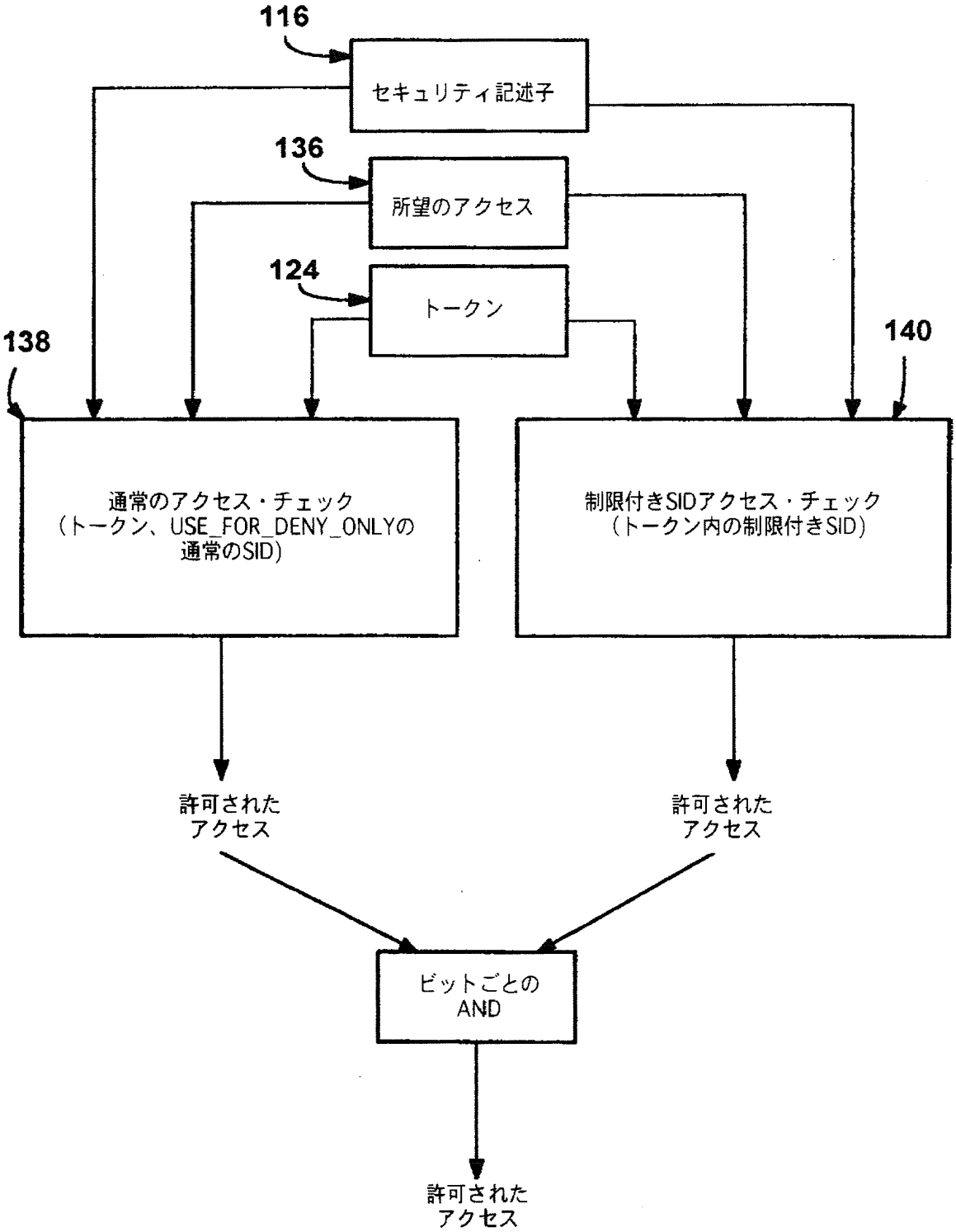


図10から
1020
RestrictedSidsが
入力フィールドに
存在するか？
Yes
No
1022
API IsTokenRestrictedを
呼び出す
1024
親トークンは
制限付きか？
Yes
No
1026
親トークンおよび
RestrictedSids入力フィールド（交差）
の両方にリストされているSIDを、
新しいトークンの
RestrictedSids入力フィールド
に入れる
1028
RestrictedSids
入力フィールド内にリスト
されているSIDを、新しい
トークンのRestrictedSids
フィールドに入れる
1030
新しいトークンの親トークンIDを、
親トークンのトークンIDに
設定する
終了

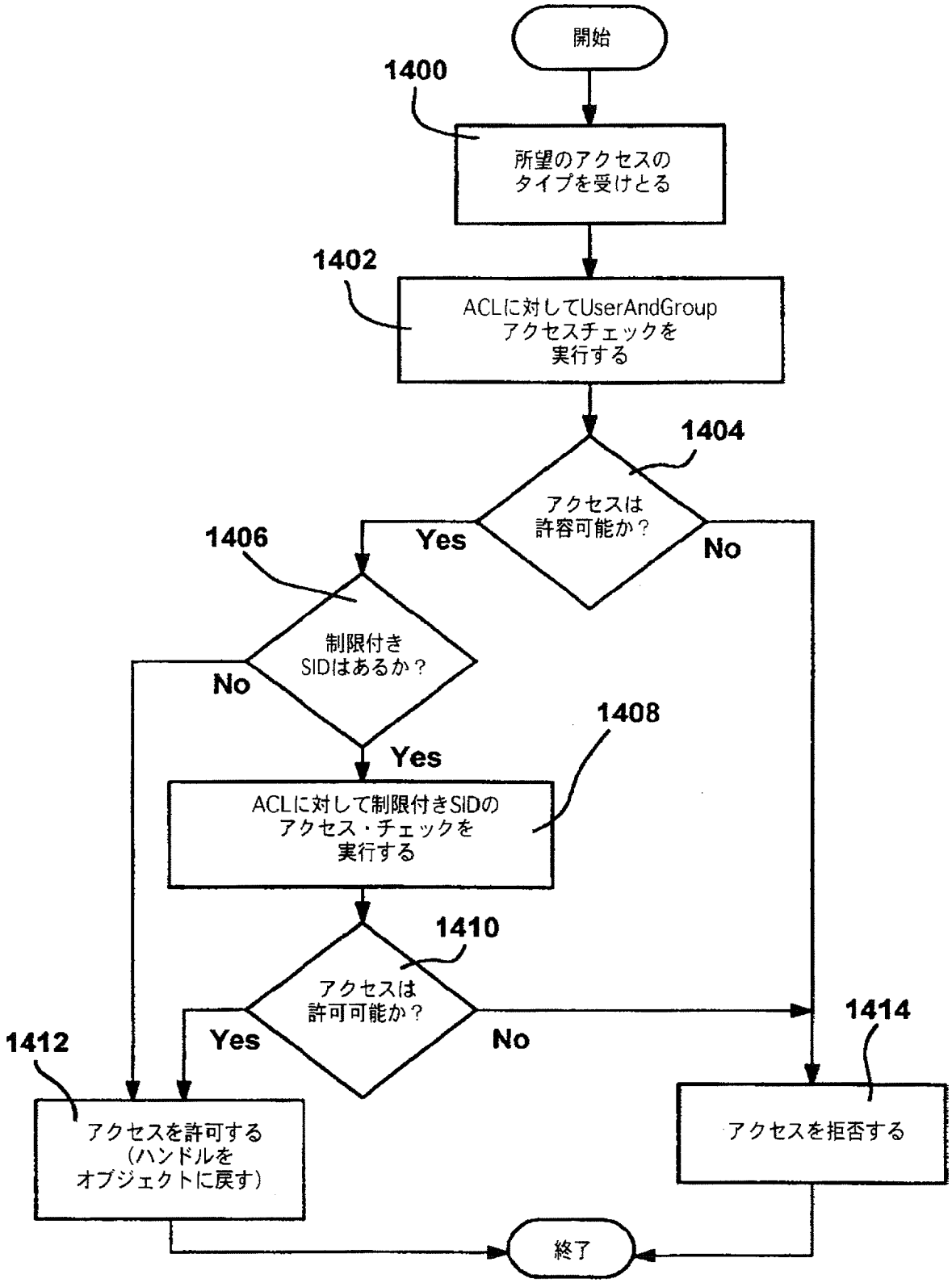
【図１２】


124
112
オブジェクト
制限付きトークン
120
ACL
ユーザ ID:
VBaker
128
XJones (DENY ALL)
SJohnson (RO)
VBaker (WR, SYNC)
チーム1 (RO)
チーム2 (RO, SYNC)
会計 (WR, SYNC)
企業 (WR, SYNC)
財務 (RO, SYNC)
Local_Machine
Local_Intranet
グループ IDs:
チーム 1
会計
バスケット・ボール(DENY)
企業
130
特権:
システムクロックの設定する
132
制限付きSID:
RAS
プロセス
134
114
(アクセス)
(オブジェクトID)
(結果)
オブジェクト
マネジャ
セキュリティ
機構
118

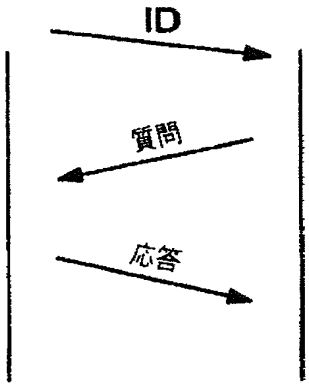
【図１３】


116
セキュリティ記述子
136
所望のアクセス
124
トークン
138
140
通常のアクセス・チェック
（トークン、USE_FOR_DENY_ONLYの
通常のSID）
制限付きSIDアクセス・チェック
（トークン内の制限付きSID）
許可された
アクセス
許可された
アクセス
ビットごとの
AND
許可された
アクセス

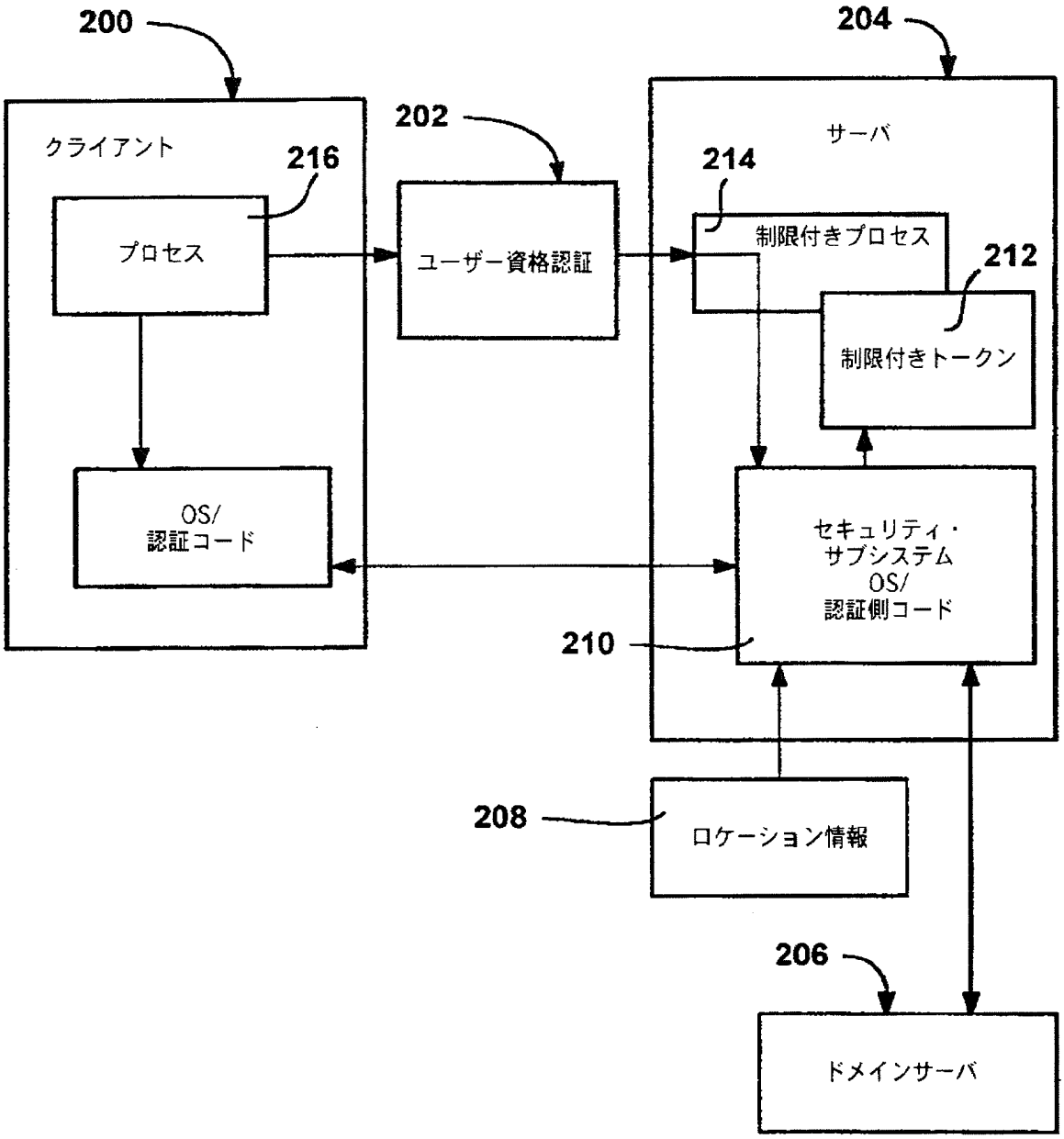
【図１４】


開始
1400
所望のアクセスの
タイプを受けとる
1402
ACLに対してUserAndGroup
アクセスチェックを
実行する
1404
アクセスは
許容可能か？
Yes
No
1406
制限付き
SIDはあるか？
No
Yes
1408
ACLに対して制限付きSIDの
アクセス・チェックを
実行する
1410
アクセスは
許可可能か？
Yes
No
1412
アクセスを許可する
（ハンドルを
オブジェクトに戻す）
1414
アクセスを拒否する
終了

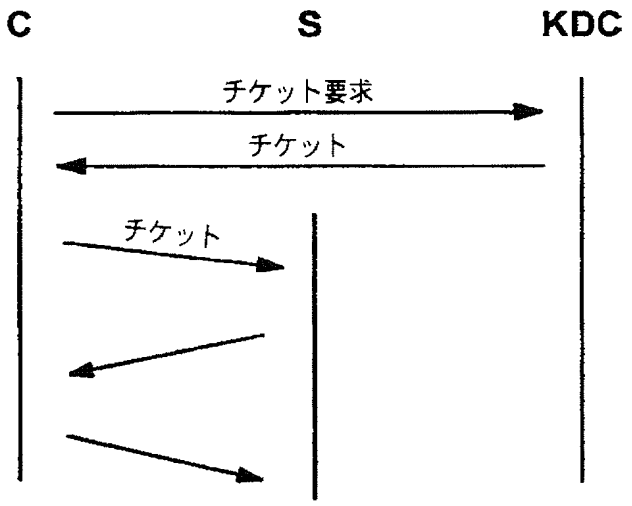
【図１５】



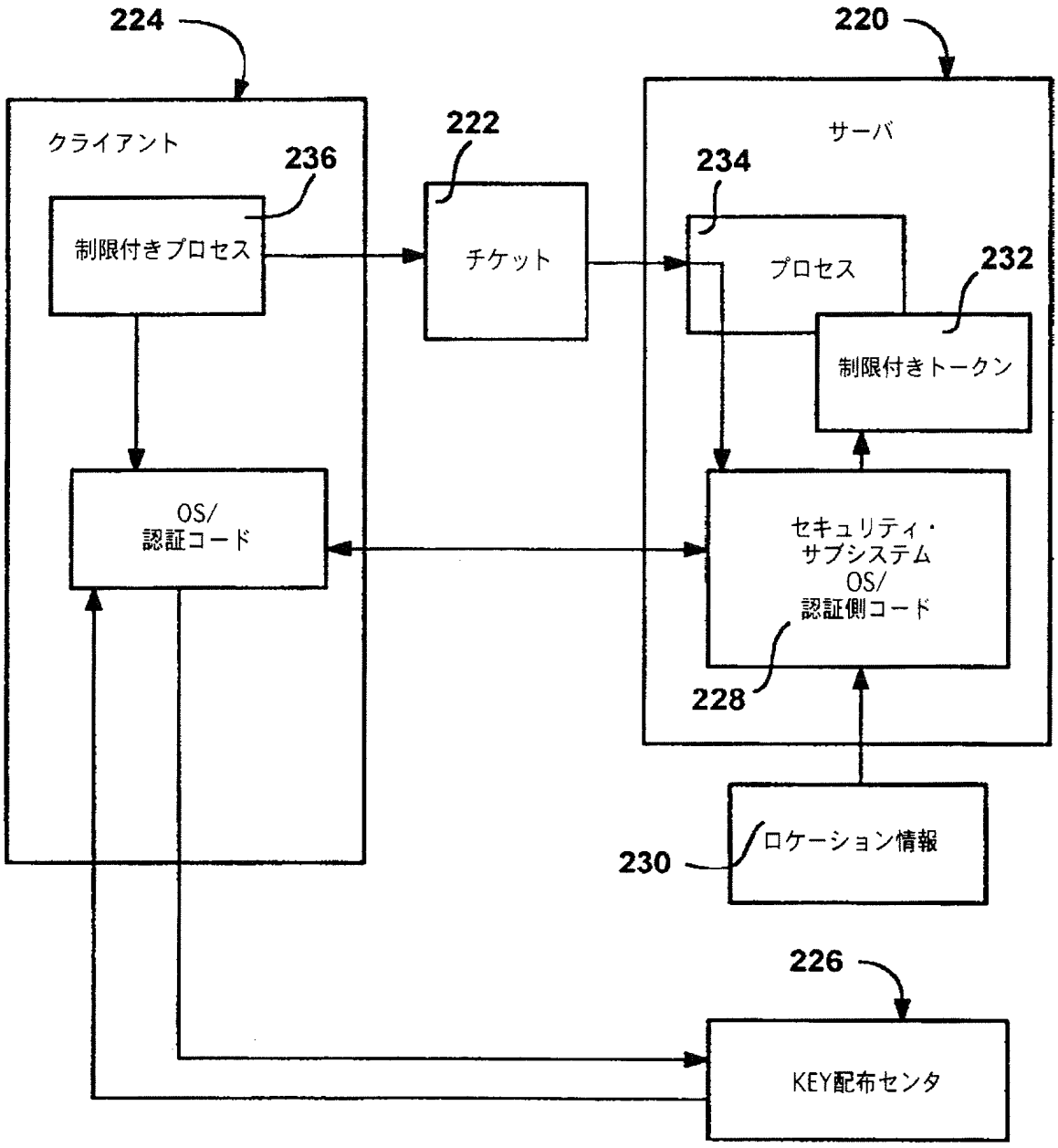
【図１６】


200
204
クライアント
216
202
サーバ
214
プロセス
ユーザー資格認証
制限付きプロセス
212
制限付きトークン
OS/
認証コード
セキュリティ・
サブシステム
OS/
認証側コード
210
208
ロケーション情報
206
ドメインサーバ

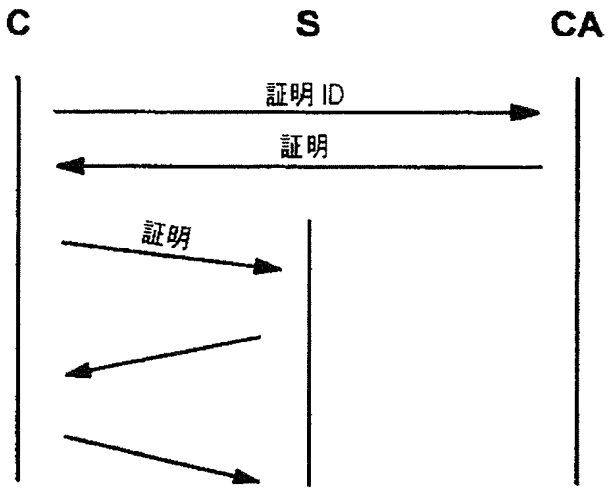
【図１７】



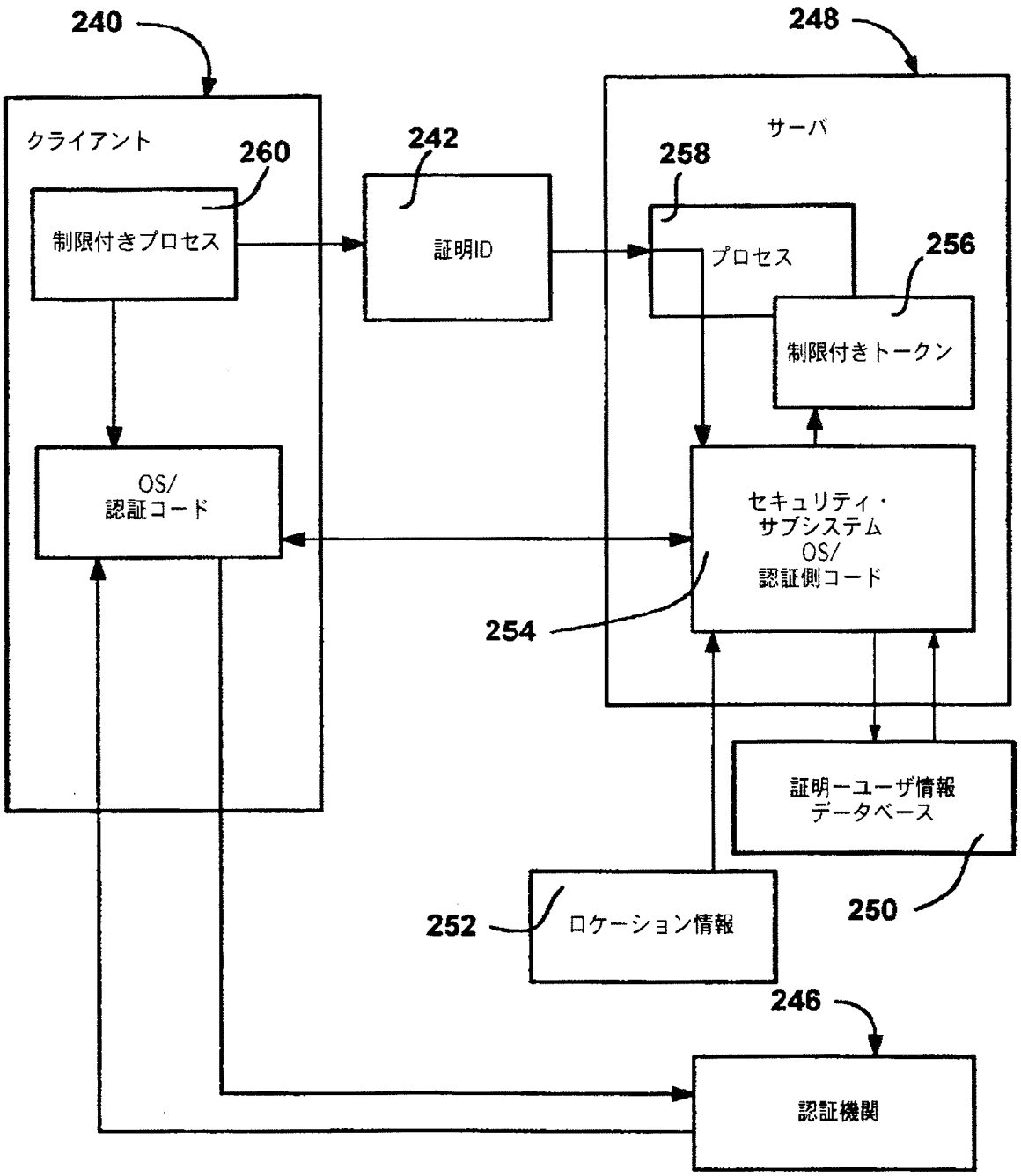
【図１８】


224
220
クライアント
236
222
サーバ
234
制限付きプロセス
チケット
プロセス
232
制限付きトークン
OS/
認証コード
セキュリティ・
サブシステム
OS/
認証側コード
228
230
ロケーション情報
226
KEY配布センタ

【図１９】



【図２０】


240
248
クライアント
260
242
サーバ
258
制限付きプロセス
証明ID
プロセス
256
制限付きトークン
OS/
認証コード
セキュリティ・
サブシステム
OS/
認証側コード
254
証明ーユーザ情報
データベース
250
252
ロケーション情報
246
認証機関

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/US 99/12913

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 05549 A (SHIVA CORPORATION) 22 February 1996 (1996-02-22) page 8, line 9 -page 9, line 12	1,21,34
A	EP 0 465 016 A (DIGITAL EQUIPMENT CORPORATION) 8 January 1992 (1992-01-08) column 4, line 26 -column 5, line 28	1,21,34

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 October 1999	18/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ströbeck, A

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/US 99/12913

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9605549 A	22-02-1996	AU 3099295 A	07-03-1996
		CA 2197219 A	22-02-1996
		DE 69510551 D	05-08-1999
		EP 0775341 A	28-05-1997
EP 0465016 A	08-01-1992	US 5204961 A	20-04-1993
		CA 2044003 A,C	26-12-1991
		DE 69130657 D	04-02-1999
		DE 69130657 T	22-07-1999
		JP 1996980 C	08-12-1995
		JP 6095991 A	08-04-1994
		JP 7031648 B	10-04-1995

フロントページの続き

(72)発明者 スージ イー. ストロム
アメリカ合衆国 98053 ワシントン州
レッドモンド ノースイースト 239 ア
ベニュー 413
(72)発明者 プラエリット ガーグ
アメリカ合衆国 98034 ワシントン州
カークランド ノースイースト 104 ア
ベニュー 12648
(72)発明者 バーラト シャー
アメリカ合衆国 98059 ワシントン州
ニューキャッスル サウスイースト 136
アベニュー 8223

Fターム(参考) 5B085 AE06 BC02